Instalar y configurar el plano de control de vSphere IaaS

Actualización 3

VMware vSphere 8.0

VMware vCenter 8.0

VMware ESXi 8.0

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware by Broadcom en:

https://docs.vmware.com/es/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contenido

Instalar y configurar el plano de control de IaaS de vSphere

Instalar y configurar el plano de control de IaaS de vSphere proporciona información sobre la configuración y administración de vSphere IaaS control plane, antes conocido como vSphere with Tanzu, mediante vSphere Client.

Instalar y configurar el plano de control de IaaS de vSphere proporciona instrucciones para habilitar vSphere IaaS control plane en clústeres de vSphere existentes, así como para crear y administrar espacios de nombres. Esta información también proporciona directrices para establecer una sesión con el plano de control de Kubernetes a través de kubectl.

Audiencia prevista

Instalar y configurar el plano de control de IaaS de vSphere se diseñó para los administradores de vSphere que deseen habilitar vSphere IaaS control plane en vSphere, así como configurar y proporcionar espacios de nombres a los equipos de desarrollo y operaciones. Los administradores de vSphere que deseen usar vSphere IaaS control plane deben tener conocimientos básicos sobre contenedores y Kubernetes.

Información actualizada

Esta documentación sobre *Instalar y configurar el plano de control de IaaS de vSphere* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de la documentación sobre *Instalar y configurar el plano de control de IaaS de vSphere*.

Revisión	Descripción
25 de junio de 2024	Actualizaciones y mejoras generales para la versión vSphere 8.0 Update 3.
18 de marzo de 2024	Se ha actualizado el tema de Reemplazar el certificado VIP para conectarse de forma segura al endpoint de API de Supervisor con una nota sobre la importación de toda la cadena de certificados.
29 de febrero de 2024	■ Se han agregado pasos para crear una nube personalizada durante la configuración inicial del controlador. Consulte Configurar el controlador. ■ Se han agregado pasos para seleccionar la nube al implementar el Supervisor. Consulte Implementar un Supervisor de tres zonas con la pila de redes de VDS y Implementar un Supervisor de una sola zona con la pila de redes de VDS. ■ Se han agregado pasos para configurar el inicio de sesión de FQDN con el Supervisor. Consulte Implementar un Supervisor de tres zonas con la pila de redes de VDS, Implementar un Supervisor de una sola zona con la pila de redes de VDS y Cambiar la configuración de red de administración en un Supervisor. ■ Se ha agregado un paso para crear el segmento de superposición de NSX. Consulte Crear un segmento de vínculo superior de nivel 0 y un segmento de superposición.
24 de enero de 2024	■ Se ha actualizado Registrar la NSX Advanced Load Balancer Controller con NSX Manager con una nota sobre la configuración de DNS y NTP. ■ Se ha agregado contenido para los pasos que se deben realizar si la implementación del Supervisor no se completa y si la configuración de NSX Advanced Load Balancer no se aplica cuando se proporciona un certificado firmado por una entidad de certificación (CA) privada. Consulte La configuración de NSX Advanced Load Balancer no se aplica.
23 de diciembre de 2023	■ Se ha agregado contenido para cambiar la configuración del equilibrador de carga en un Supervisor configurado con redes VDS. Consulte Cambiar la configuración del equilibrador de carga en un Supervisor configurado con redes VDS. ■ Se ha actualizado el contenido para cambiar la configuración de redes de cargas de trabajo del Supervisor configurado con redes VDS. Consulte Cambiar la configuración de red de carga de trabajo en un Supervisor configurada con redes de VDS.
13 DEC 2023	Se agregó una referencia para preparar hosts ESXi como nodos de transporte. Consulte VDS requerido para el tráfico del nodo de transporte del host.
21 de noviembre de 2023	Se ha actualizado la documentación para indicar que no se admiten varias NSX en el clúster supervisor. Consulte Agregar un administrador de equipo.

Revisión	Descripción
29 de septiembre de 2023	■ Actualizaciones en Configuración de los ajustes del proxy HTTP en vSphere IaaS control plane. ■ Se han actualizado los requisitos para personalizar el equilibrador de carga de HAProxy. Consulte Personalizar el equilibrador de carga de HAProxy. .
21 de septiembre de 2023	Se actualizó la sección de redes con información para instalar y configurar NSX Advanced Load Balancer con NSX. Consulte Instalar y configurar NSX y NSX Advanced Load Balancer.
30 de junio de 2023	Se agregaron los tamaños del plano de control de Supervisor en los temas de instalación de Supervisor y Cambiar el tamaño del plano de control de un Supervisor.
23 de junio de 2023	Se actualizó un vínculo para crear y editar bibliotecas de contenido. Consulte Importar el archivo OVA de NSX Advanced Load Balancer en una biblioteca de contenido local.
15 de junio de 2023	Se agregó una nota donde se indica que solo puede utilizar un proxy HTTP para registrar un Supervisor con Tanzu Mission Control. Consulte Configuración de los ajustes del proxy HTTP en vSphere IaaS control plane.
15 de mayo de 2023	Se agregó una nota donde se indica que no debe habilitar el dominio de consumo en las directivas de almacenamiento que se utilizan para un Supervisor o un espacio de nombres en un Supervisor de una zona. Consulte Capítulo 2 Crear directivas de almacenamiento para vSphere IaaS control plane.
12 de mayo de 2023	Se agregó una nota para indicar que si actualizó el entorno de vSphere IaaS control plane desde una versión de vSphere anterior a la versión 8.0 y desea utilizar zonas de vSphere, debe crear un nuevo Supervisor de tres zonas. Consulte Capítulo 5 Implementar Supervisor de tres zonas .
26 de abril de 2023	Se ha movido Configurar y administrar espacios de nombre de vSphere a *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.
18 de abril de 2023	Se actualizó la sección Instalar y configurar el NSX Advanced Load Balancer para incluir la compatibilidad con NSX Advanced Load Balancer versión 22.1.3.

Instalación y flujo de trabajo de vSphere IaaS control plane

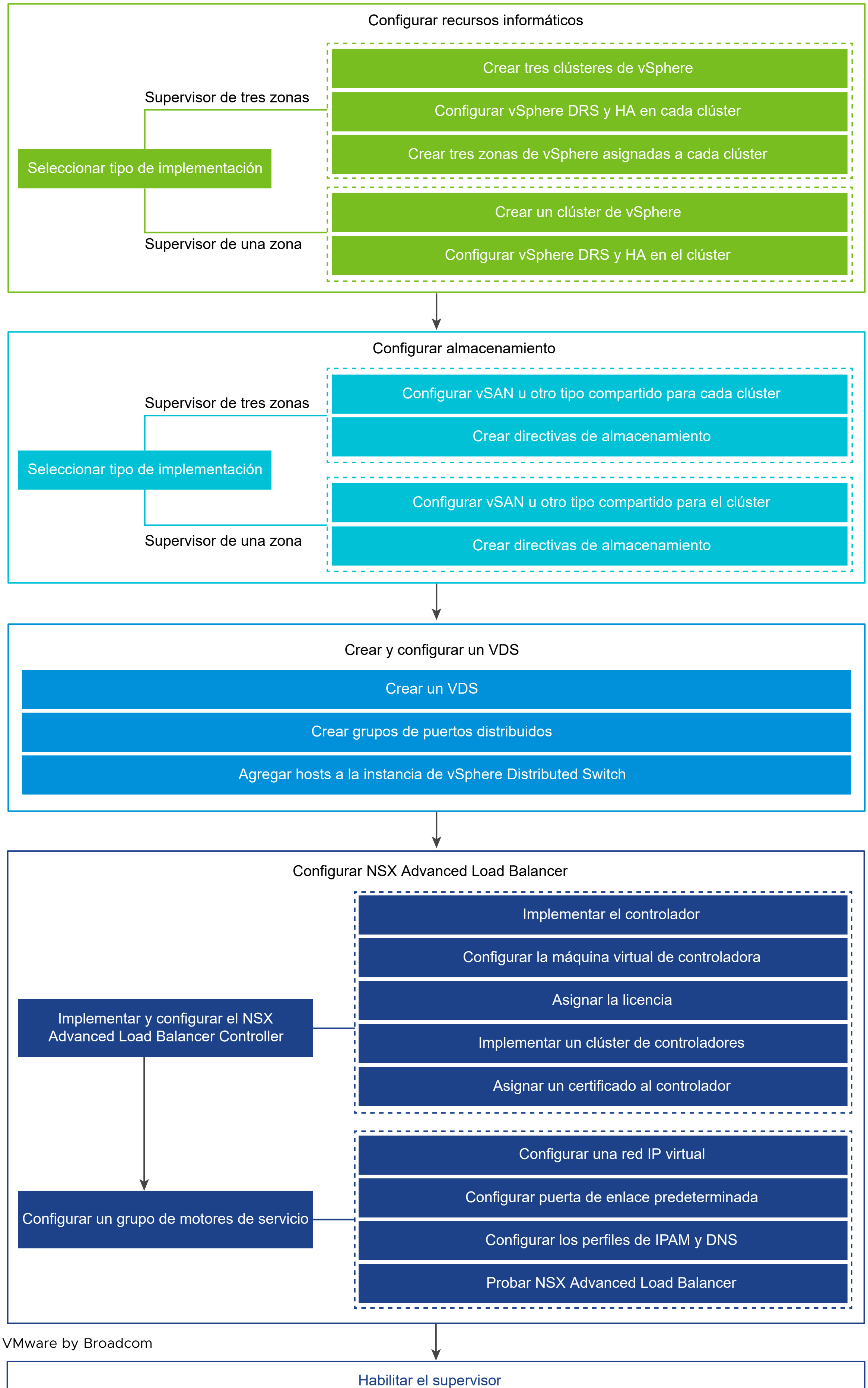
1

Revise los flujos de trabajo para convertir los clústeres de vSphere en una plataforma para ejecutar cargas de trabajo de Kubernetes en vSphere.

Flujo de trabajo para implementar un Supervisor con redes de VDS y NSX Advanced Load Balancer

Como administrador de vSphere, puede implementar un Supervisor con la pila de redes basada en redes de VDS mediante NSX Advanced Load Balancer.

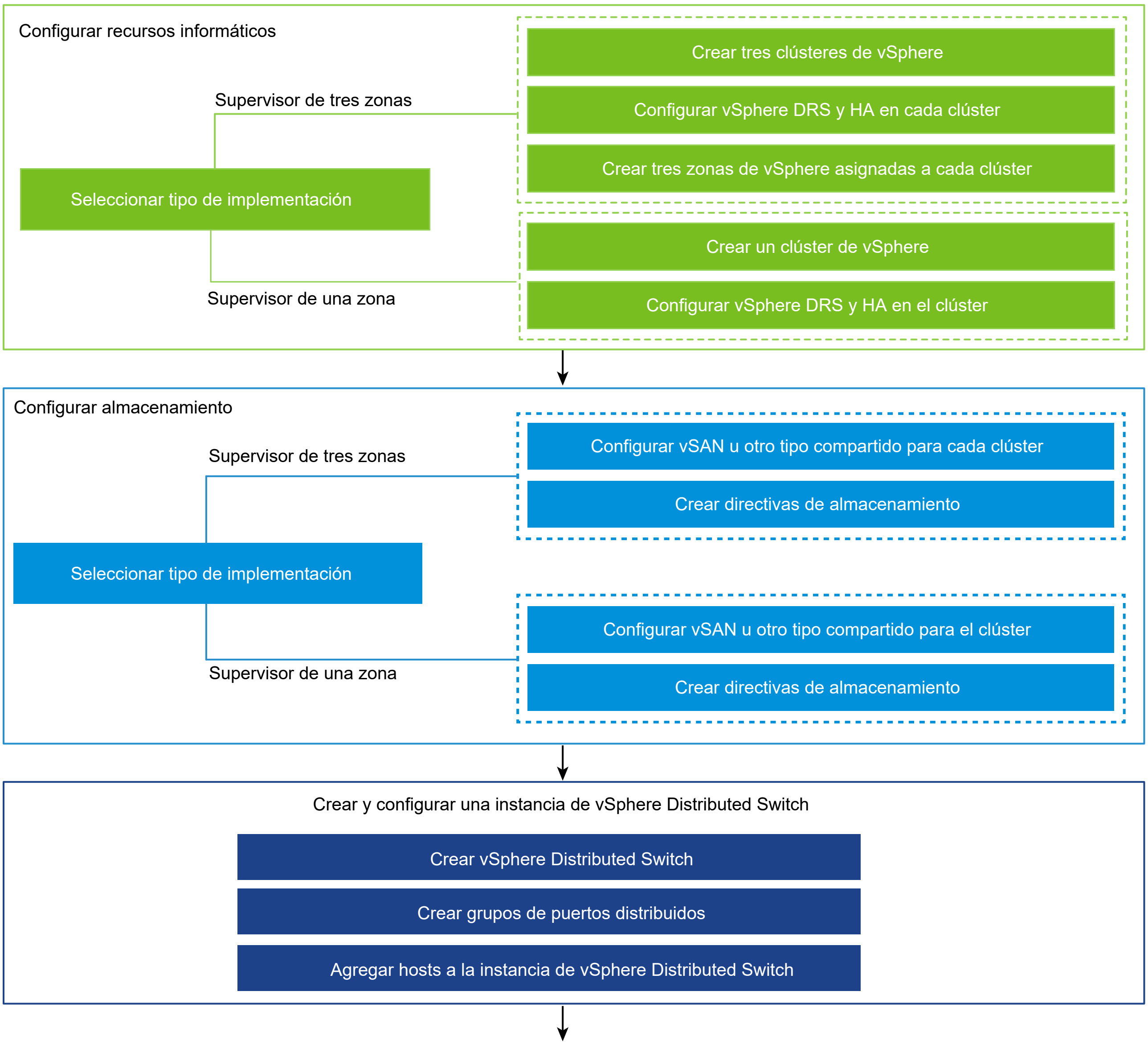
Figura 1-1. Flujo de trabajo para implementar un supervisor con NSX Advanced Load Balancer

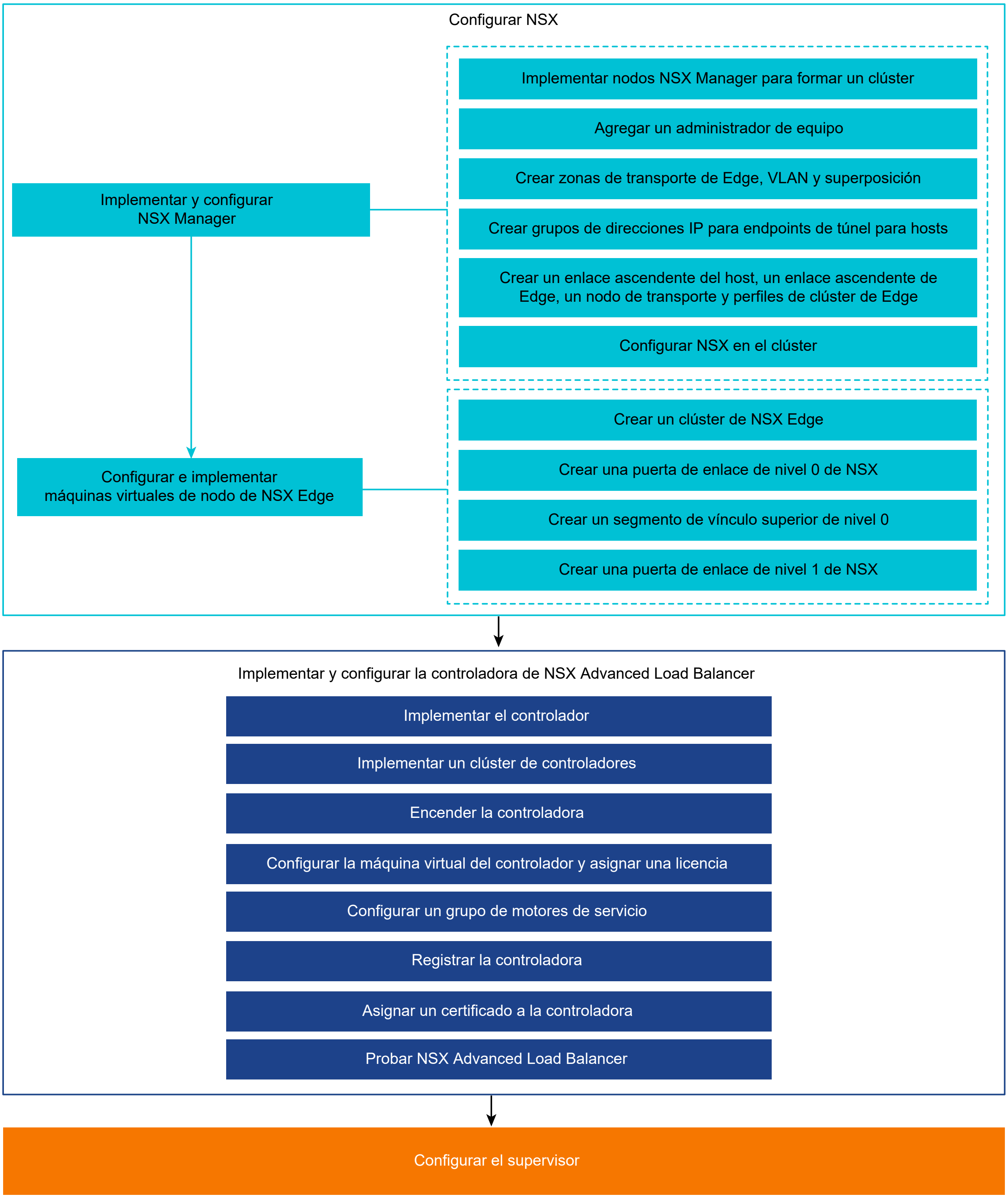


Supervisor con redes de NSX y flujo de trabajo de la NSX Advanced Load Balancer Controller

Como administrador de vSphere, puede implementar un Supervisor con la pila de redes NSX y la NSX Advanced Load Balancer Controller.

Figura 1-2. Flujo de trabajo para implementar un supervisor con redes NSX y NSX Advanced Load Balancer Controller

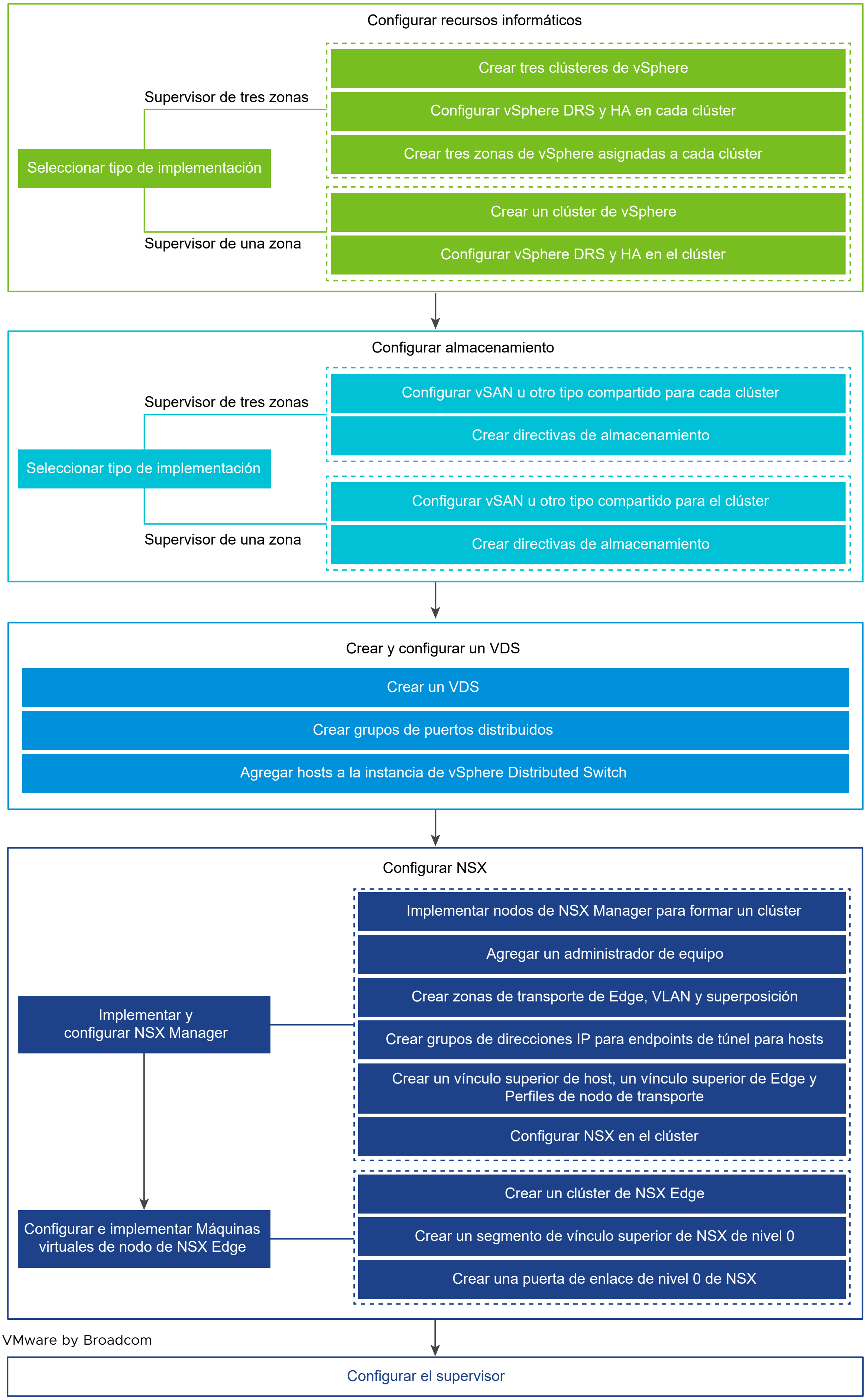



Configurar NSX
Implementar y configurar NSX Manager
Implementar nodos NSX Manager para formar un clúster
Agregar un administrador de equipo
Crear zonas de transporte de Edge, VLAN y superposición
Crear grupos de direcciones IP para endpoints de túnel para hosts
Crear un enlace ascendente del host, un enlace ascendente de Edge, un nodo de transporte y perfiles de clúster de Edge
Configurar NSX en el clúster
Configurar e implementar máquinas virtuales de nodo de NSX Edge
Crear un clúster de NSX Edge
Crear una puerta de enlace de nivel 0 de NSX
Crear un segmento de vínculo superior de nivel 0
Crear una puerta de enlace de nivel 1 de NSX
Implementar y configurar la controladora de NSX Advanced Load Balancer
Implementar el controlador
Implementar un clúster de controladores
Encender la controladora
Configurar la máquina virtual del controlador y asignar una licencia
Configurar un grupo de motores de servicio
Registrar la controladora
Asignar un certificado a la controladora
Probar NSX Advanced Load Balancer
Configurar el supervisor

Flujo de trabajo para implementar un Supervisor con redes de NSX

Como administrador de vSphere, puede implementar un Supervisor con la pila de redes basada en NSX.

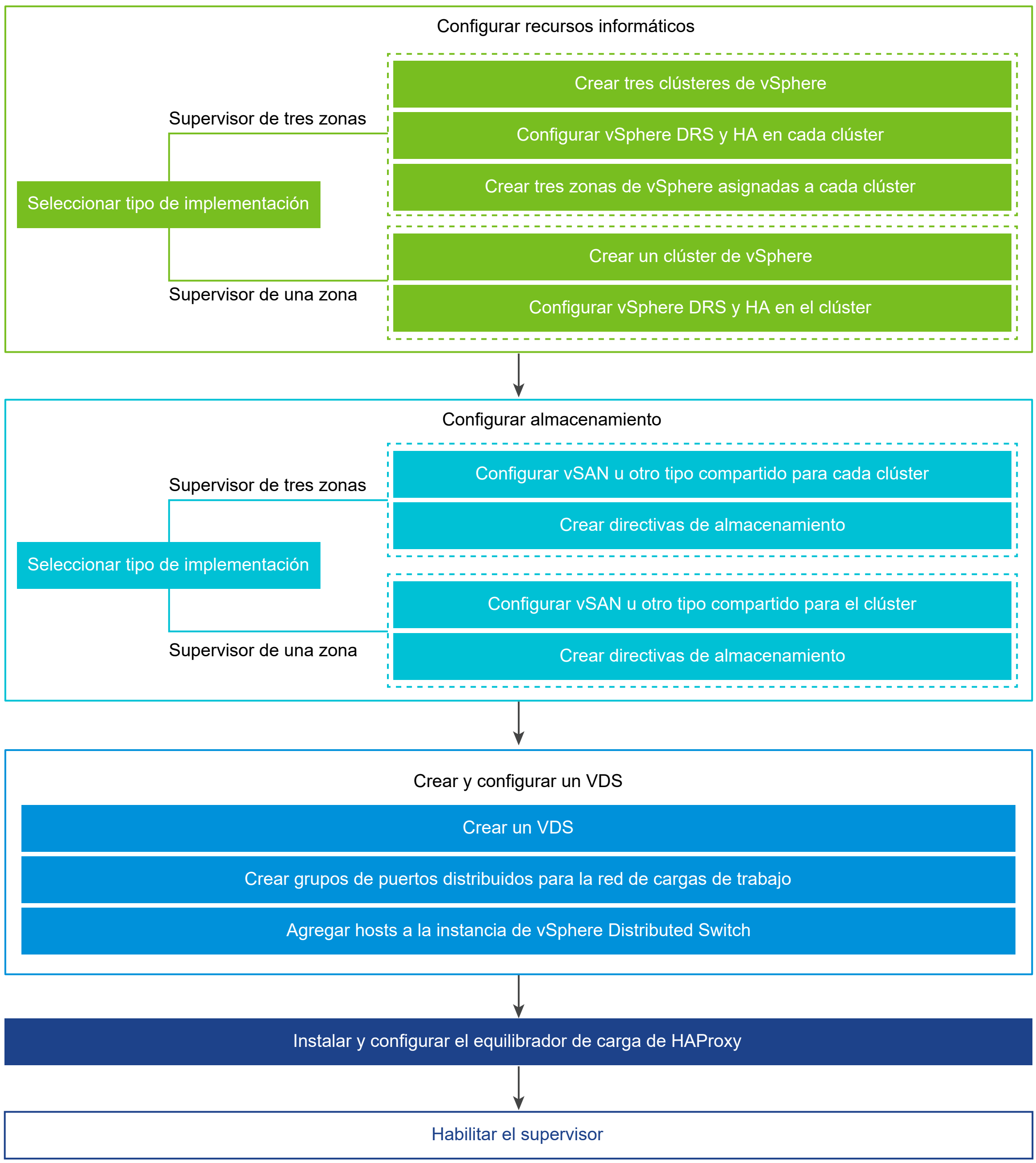
Figura 1-3. Flujo de trabajo para implementar un supervisor con NSX como pila de redes



Flujo de trabajo para implementar un Supervisor con redes de VDS y el equilibrador de carga de HAProxy

Como administrador de vSphere, puede implementar un Supervisor con la pila de redes basada en VDS y el equilibrador de carga de HAProxy.

Figura 1-4. Flujo de trabajo para implementar un supervisor con redes de VDS y HAProxy



Lea los siguientes temas a continuación:

- Requisitos previos para configurar vSphere IaaS control plane en clústeres de vSphere

Requisitos previos para configurar vSphere IaaS control plane en clústeres de vSphere

Verifique los requisitos previos para habilitar vSphere IaaS control plane en su entorno de vSphere. Para ejecutar cargas de trabajo basadas en contenedores de forma nativa en vSphere, como administrador de vSphere, habilite los clústeres de vSphere como Supervisores. Un Supervisor contiene una capa de Kubernetes que permite ejecutar cargas de trabajo de Kubernetes en vSphere mediante la implementación de pods de vSphere, así como aprovisionar máquinas virtuales y clústeres de Tanzu Kubernetes.

Crear y configurar clústeres de vSphere

Un Supervisor puede ejecutarse en uno o tres clústeres de vSphere asociados con zonas de vSphere. Cada zona de vSphere se asigna a un clúster de vSphere y es posible implementar un Supervisor en una o tres zonas. Un Supervisor de tres zonas aumenta la cantidad de recursos disponibles para ejecutar cargas de trabajo de Kubernetes y su alta disponibilidad en el nivel de clúster de vSphere permite proteger las cargas de trabajo contra los errores del clúster. Un Supervisor de una zona obtiene alta disponibilidad de nivel de host a través de vSphere HA y utiliza los recursos de un solo clúster para ejecutar las cargas de trabajo de Kubernetes.

Nota Una vez que implemente un Supervisor en una zona de vSphere, no podrá expandir el Supervisor a una implementación de tres zonas.

Cada clúster de vSphere en el que se desee implementar un Supervisor debe cumplir con los siguientes requisitos:

- Cree y configure un clúster de vSphere con al menos dos hosts ESXi. Si utiliza vSAN, el clúster debe tener al menos tres hosts o cuatro para alcanzar un rendimiento óptimo. Consulte Crear y configurar clústeres.
- Configure el clúster con almacenamiento compartido, como vSAN. Se requiere almacenamiento compartido para vSphere HA, DRS y para almacenar volúmenes contenedores persistentes. Consulte Crear un clúster de vSAN .
- Habilite el clúster con vSphere HA. Consulte Crear y usar clústeres de vSphere HA.
- Habilite el clúster con vSphere DRS en modo totalmente automatizado. Consulte Crear un clúster de DRS.
- Compruebe que la cuenta de usuario tenga el privilegio **Modificar configuración de todo el clúster** en el clúster de vSphere para poder implementar el Supervisor.
- Para implementar un Supervisor de tres zonas, cree tres zonas de vSphere. Consulte Capítulo 3 Crear zonas de vSphere para una implementación de Supervisor de varias zonas.
- Si desea utilizar imágenes de vSphere Lifecycle Manager con el Supervisor, cambie los clústeres de vSphere en los que desea activar **Administración de cargas de trabajo** para utilizar imágenes de vSphere Lifecycle Manager antes de activar **Administración de cargas de trabajo**. Puede administrar el ciclo de vida de un Supervisor con líneas base de

vSphere Lifecycle Manager o con imágenes de vSphere Lifecycle Manager. Sin embargo, no puede convertir un Supervisor que utilice líneas base de vSphere Lifecycle Manager en un Supervisor que utilice imágenes de vSphere Lifecycle Manager. Por lo tanto, es necesario cambiar los clústeres de vSphere para usar imágenes de vSphere Lifecycle Manager antes de activar **Administración de cargas de trabajo**.

Crear directivas de almacenamiento

Antes de implementar un Supervisor, debe crear directivas de almacenamiento que determinen la colocación del almacén de datos de las máquinas virtuales del plano de control de Supervisor. Si el Supervisor admite pods de vSphere, también necesitará directivas de almacenamiento para los contenedores y las imágenes. Puede crear directivas de almacenamiento asociadas con diferentes niveles de servicios de almacenamiento.

Consulte Capítulo 2 Crear directivas de almacenamiento para vSphere IaaS control plane.

Elegir y configurar la pila de redes

Para implementar un Supervisor, debe configurar la pila de redes para usarla con este. Tiene dos opciones: redes de NSX o vSphere Distributed Switch (vDS) con un equilibrador de carga. Puede configurar el NSX Advanced Load Balancer o el equilibrador de carga de HAProxy.

Para usar las redes de NSX para el Supervisor:

- Revise los requisitos del sistema y las topologías para las redes de NSX. Consulte Requisitos para habilitar un supervisor de tres zonas con NSX y Requisitos para configurar un supervisor de clúster único con NSX en *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Instale y configure NSX para vSphere IaaS control plane. Consulte Instalar y configurar NSX para vSphere IaaS control plane.

Para utilizar las redes de vDS con NSX Advanced Load Balancer en el Supervisor:

- Revise los requisitos de NSX Advanced Load Balancer. Consulte Requisitos para un supervisor de tres zonas con NSX Advanced Load Balancer y Requisitos para habilitar un supervisor de clúster único con NSX Advanced Load Balancer en *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Cree una instancia de vSphere Distributed Switch (vDS), agregue todos los hosts ESXi del clúster a vDS y cree grupos de puertos para las redes de cargas de trabajo. Consulte Crear una instancia de vSphere Distributed Switch para un Supervisor para su uso con NSX Advanced Load Balancer.
- Implemente y configure el NSX Advanced Load Balancer. Consulte Implementar el controlador de NSX Advanced Load Balancer.

Nota vSphere IaaS control plane admite NSX Advanced Load Balancer con vSphere 7 U2 y versiones posteriores.

Para utilizar las redes de vDS con el equilibrio de carga de HAProxy en el Supervisor:

- Revise los requisitos del sistema y las topologías de red para las redes de vSphere con un equilibrador de carga de HAProxy. Consulte Requisitos para habilitar un supervisor de tres zonas con el equilibrador de carga de HAProxy y Requisitos para habilitar un supervisor de clúster único con redes de VDS y el equilibrador de carga de HAProxy *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Cree una instancia de vSphere Distributed Switch (VDS), agregue todos los hosts ESXi del clúster a vDS y cree grupos de puertos para las redes de cargas de trabajo. Consulte Crear una instancia de vSphere Distributed Switch para un Supervisor para su uso con el equilibrador de carga de HAProxy.
- Instale y configure la instancia de equilibrador de carga de HAProxy que se puede enrutar al vDS conectado a los hosts desde los clústeres de vSphere donde se implementó el Supervisor. El equilibrador de carga de HAProxy admite la conectividad de red con las cargas de trabajo de las redes de clientes y para equilibrar la carga del tráfico entre los clústeres de Tanzu Kubernetes. Consulte Instalar y configurar el equilibrador de carga de HAProxy.

Nota vSphere IaaS control plane admite el equilibrador de carga de HAProxy con vSphere 7 U1 y versiones posteriores.

Crear directivas de almacenamiento para vSphere IaaS control plane

2

Antes de habilitar vSphere IaaS control plane, cree las directivas de almacenamiento que se utilizarán en el Supervisor y los espacios de nombres. Las directivas representan almacenes de datos y administran la colocación del almacenamiento de componentes y objetos como máquinas virtuales del plano de control de Supervisor, discos efímeros de pod de vSphere e imágenes de contenedor. Es posible que también necesite directivas para la colocación del almacenamiento de los volúmenes persistentes y las bibliotecas de contenido de máquina virtual. Si utiliza clústeres de Tanzu Kubernetes, las directivas de almacenamiento también determinan cómo se implementan los nodos del clúster de Tanzu Kubernetes.

Según el entorno de almacenamiento de vSphere y las necesidades de desarrollo y operaciones, puede crear varias directivas de almacenamiento para diferentes clases de almacenamiento. Por ejemplo, si su entorno de almacenamiento de vSphere tiene tres clases de almacenes de datos (Bronce, Plata y Oro), puede crear directivas de almacenamiento para todos los tipos almacenes de datos.

Cuando se habilita un Supervisor y se configuran espacios de nombres, es posible asignar diferentes directivas de almacenamiento para que las utilicen diversos objetos, componentes y cargas de trabajo.

Nota Las directivas de almacenamiento que se crean para un Supervisor o para un espacio de nombres en un Supervisor de una sola zona no necesitan tener en cuenta la topología. No habilite el dominio de uso para esas directivas.

Las directivas de almacenamiento que se crean para un espacio de nombres en un Supervisor de tres zonas deben reconocer la topología y tener el dominio de uso habilitado en el paso 4b. El espacio de nombres de tres zonas impide que se asignen directivas de almacenamiento que no reconozcan la topología.

El siguiente ejemplo crea la directiva de almacenamiento para el almacén de datos etiquetado como Oro.

Requisitos previos

- Para familiarizarse con la información sobre las directivas de almacenamiento en vSphere IaaS control plane, consulte Acerca de las directivas de almacenamiento en *Planificación y conceptos del plano de control de IaaS de vSphere*.

- Si utiliza la plataforma persistencia de datos de vSAN para el almacenamiento persistente y necesita crear directivas de almacenamiento personalizadas para almacenes de datos SNA de vSAN Direct o vSAN, consulte Crear directivas de almacenamiento personalizadas para la plataforma de persistencia de datos de vSAN en *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.
- Si necesita crear directivas de almacenamiento con reconocimiento de topología para usarlas para el almacenamiento persistente en un Supervisor de tres zonas, familiarícese con las directrices de Usar almacenamiento persistente en un supervisor de tres zonas en *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.
- Asegúrese de que el almacén de datos al que hace referencia en la directiva de almacenamiento se comparta entre todos los hosts de ESXi del clúster. Se admiten todos los almacenes de datos compartidos del entorno, incluidos VMFS, NFS, vSAN o vVols.
- Privilegios necesarios: **Directivas de almacenamiento de VM. Actualizar** y **Directivas de almacenamiento de VM. Ver**.

Procedimiento

1 Agregue etiquetas al almacén de datos.

   a Haga clic con el botón derecho en el almacén de datos que desea etiquetar y seleccione **Etiquetas y atributos personalizados > Asignar etiqueta**.

   b Haga clic en **Agregar etiqueta** y especifique las propiedades de la etiqueta.

Propiedad	Descripción
Nombre	Especifique el nombre de la etiqueta del almacén de datos, por ejemplo, **`Oro`**.
Descripción	Agregue la descripción de la etiqueta. Por ejemplo, **`Almacén de datos para objetos de Kubernetes`**.
Categoría	Seleccione una categoría existente o cree una categoría nueva. Por ejemplo, **`Almacenamiento para Kubernetes`**.

2 En vSphere Client, abra el asistente **Crear directiva de almacenamiento de máquina virtual**.

   a Haga clic en **Menú > Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

   c Haga clic en **Crear directiva de almacenamiento de máquina virtual**.

3 Introduzca el nombre y la descripción de la directiva.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento (por ejemplo, `goldsp`). **Nota** Cuando vSphere IaaS control plane convierte las directivas de almacenamiento que se asignan a espacios de nombres en clases de almacenamiento de Kubernetes, cambia todas las letras mayúsculas a minúsculas y reemplaza los espacios por guiones (-). Para evitar confusiones, utilice minúsculas y no use espacios en los nombres de las directivas de almacenamiento de máquina virtual.
Descripción	Introduzca la descripción de la directiva de almacenamiento.

4 En la página **Estructura de directiva**, seleccione las siguientes opciones y haga clic en **Siguiente**.

   a En **Reglas específicas de almacenes datos**, habilite las reglas de colocación basadas en etiquetas.

   b Para crear una directiva con reconocimiento de topología, en **Topología de almacenamiento**, seleccione **Habilitar dominio de consumo**.

   Este paso solo es necesario si planea crear directivas con reconocimiento de topología que se utilizarán para el almacenamiento persistente en un espacio de nombres en un Supervisor de tres zonas.

5 En la página **Colocación basada en etiquetas**, cree las reglas de la etiqueta.

Seleccione las opciones en función del siguiente ejemplo.

Opción	Descripción
Categoría de etiqueta	En el menú desplegable, seleccione la categoría de la etiqueta, por ejemplo, **Almacenamiento para Kubernetes**.
Opción de uso	Seleccione **Usar almacenamiento etiquetado con**.
Etiquetas	Haga clic en **Examinar etiquetas** y seleccione la etiqueta del almacén de datos, por ejemplo, **Oro**.

6 Si habilitó **Topología de almacenamiento**, en la página **Dominio de consumo**, especifique el tipo de topología de almacenamiento.

Opción	Descripción
Zonal	El almacén de datos se comparte entre todos los hosts de una sola zona.

7 En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos que coinciden con esta directiva.

En este ejemplo, solo se muestra el almacén de datos etiquetado como Oro.

8 En la página **Revisar y finalizar**, revise la configuración de la directiva de almacenamiento y haga clic en **Finalizar**.

Resultados

Se mostrará la nueva directiva de almacenamiento para el almacén de datos etiquetado como Oro en la lista de directivas de almacenamiento existentes.

Pasos siguientes

Después de crear las directivas de almacenamiento, un administrador de vSphere puede realizar las siguientes tareas:

- Asignar las directivas de almacenamiento al Supervisor. Las directivas de almacenamiento configuradas en el Supervisor garantizan que las máquinas virtuales de plano de control, los discos efímeros del pod y las imágenes de contenedor se coloquen en los almacenes de datos que representan las directivas.
- Asignar las directivas de almacenamiento al espacio de nombres de vSphere. Las directivas de almacenamiento visibles para el espacio de nombres determinan a qué almacenes de datos pueden acceder al espacio de nombres y cuáles pueden utilizar para los volúmenes persistentes. Las directivas de almacenamiento aparecen como clases de almacenamiento de Kubernetes coincidentes en el espacio de nombres. También se propagan al clúster de Tanzu Kubernetes en este espacio de nombres. Los ingenieros de desarrollo y operaciones pueden utilizar las clases de almacenamiento en sus especificaciones de notificación de volúmenes persistentes. Consulte Crear y configurar un espacio de nombres de vSphere.

Crear zonas de vSphere para una implementación de Supervisor de varias zonas

3

Revise la forma de crear zonas de vSphere que puede utilizar para proporcionar alta disponibilidad de nivel de clúster a las cargas de trabajo de Kubernetes que se ejecutan en un Supervisor. Para proporcionar alta disponibilidad de nivel de clúster a las cargas de trabajo de Kubernetes, implemente el Supervisor en tres zonas de vSphere. Cada zona de vSphere se asigna a un clúster de vSphere que tiene un mínimo de 2 hosts.

Requisitos previos

- Cree tres clústeres de vSphere con al menos 3 hosts en cada zona. Para el almacenamiento con vSAN, el clúster debe tener 4 hosts.
- Configure el almacenamiento con vSAN u otra solución de almacenamiento compartido para cada clúster.
- Habilite vSphere HA y vSphere DRS en el modo Totalmente automatizado o Parcialmente automatizado.
- Configure las redes con redes NSX o vSphere Distributed Switch (vDS) para los clústeres.

Procedimiento

1. En vSphere Client, desplácese hasta vCenter Server.
2. Seleccione **Configurar** y, a continuación, **Zonas de vSphere**.
3. Haga clic en **Agregar nueva zona de vSphere**.
4. Asigne un nombre a la zona, por ejemplo, `zona1`, y agregue una descripción opcional.
5. Seleccione un clúster de vSphere para agregarlo a la zona y haga clic en **Finalizar**.
6. Repita los pasos para crear tres zonas de vSphere.

Pasos siguientes

-
  - Configure una pila de redes para usarla con el Supervisor. Consulte Capítulo 4 Redes para vSphere IaaS control plane.
  - Active el Supervisor en las tres zonas de vSphere que creó. Consulte Capítulo 5 Implementar Supervisor de tres zonas .

Si necesita realizar cambios en una zona de vSphere, puede hacerlo antes de implementar el Supervisor en la zona.

Administrar zonas de vSphere

Si necesita realizar cambios en una zona de vSphere, debe hacerlo antes de implementar un Supervisor en la zona. Puede cambiar el clúster asociado a la zona o eliminar esta última. Al eliminar una zona de vSphere, se quita su clúster asociado y, a continuación, se elimina la zona de vCenter Server.

Eliminar un clúster de una zona de vSphere

Para eliminar un clúster de una zona de vSphere, haga clic en los tres puntos (...) de la tarjeta de zona y seleccione **Quitar clúster**. El clúster se eliminará de la zona y se podrá agregar uno diferente.

Nota No se puede eliminar un clúster de una zona de vSphere si ya existe un Supervisor habilitado en esa zona.

Eliminar una zona de vSphere

Para eliminar una zona de vSphere, haga clic en los tres puntos (...) de la tarjeta de zona y seleccione **Eliminar zona**.

Nota No puede eliminar una zona de vSphere si ya existe un Supervisor habilitado en esa zona.

Redes para vSphere IaaS control plane

4

Una instancia de Supervisor puede utilizar la pila de redes de vSphere o VMware NSX® para proporcionar conectividad a las máquinas virtuales, los servicios y las cargas de trabajo del plano de control de Kubernetes. Las redes que se utilizan para los clústeres de Tanzu Kubernetes aprovisionadas por Tanzu Kubernetes Grid son una combinación del tejido que se encuentra subyacente a la infraestructura de vSphere IaaS control plane y el software de código abierto que proporciona las redes para los pods, los servicios y las entradas del clúster.

Lea los siguientes temas a continuación:

Redes del Supervisor

En un entorno de vSphere IaaS control plane, un Supervisor puede utilizar una pila de redes de vSphere o NSX para proporcionar conectividad a las cargas de trabajo, los servicios y las máquinas virtuales del plano de control del Supervisor.

Cuando se configura un Supervisor con la pila de redes de vSphere, todos los hosts del Supervisor se conectan a un vDS que proporciona conectividad a las cargas de trabajo y las máquinas virtuales del plano de control del Supervisor. Un Supervisor que utiliza la pila de redes de vSphere requiere un equilibrador de carga en la red de administración de vCenter Server que proporcione conectividad a los usuarios de desarrollo y operaciones, y a los servicios externos.

Un Supervisor que esté configurado con NSX utiliza las redes basadas en software de la solución, así como un equilibrador de carga de NSX Edge o la NSX Advanced Load Balancer para proporcionar conectividad a los servicios externos y a los usuarios de desarrollo y operaciones. Puede configurar la NSX Advanced Load Balancer en NSX si el entorno cumple las siguientes condiciones:

- La versión de NSX es 4.1.1 o posterior.
- La versión de NSX Advanced Load Balancer es la 22.1.4 o posterior con la licencia Enterprise.

- La NSX Advanced Load Balancer Controller que tiene pensado configurar se registra en NSX.
- Aún no se ha configurado un equilibrador de carga de NSX en el Supervisor.

Redes de un Supervisor con VDS

En un Supervisor respaldado por VDS como la pila de redes, todos los hosts de los clústeres de vSphere que respaldan el Supervisor deben estar conectados al mismo VDS. El Supervisor utiliza grupos de puertos distribuidos como redes de carga de trabajo para el tráfico del plano de control y las cargas de trabajo de Kubernetes. Las redes de carga de trabajo se asignan a los espacios de nombres en el Supervisor.

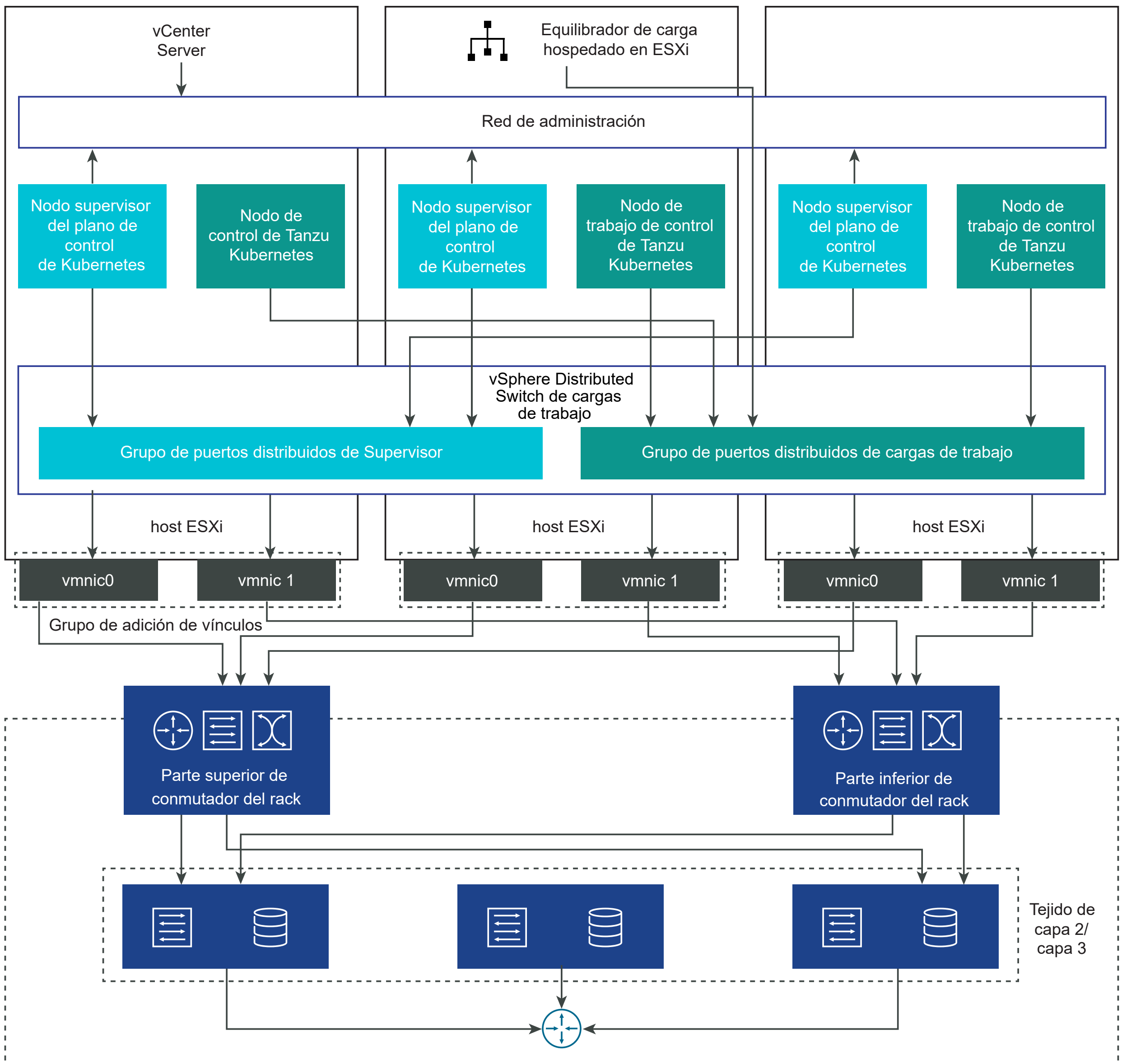
Según la topología que se implemente para el Supervisor, es posible usar uno o varios grupos de puertos distribuidos como redes de carga de trabajo. La red que proporciona conectividad a las máquinas virtuales del plano de control del Supervisor se denomina Red de carga de trabajo principal. Puede asignar esta red a todos los espacios de nombres de la instancia de Supervisor o puede utilizar diferentes redes para cada espacio de nombres. Los clústeres de Tanzu Kubernetes Grid se conectan a la red de carga de trabajo que se asigna al espacio de nombres en el que residen los clústeres.

Un Supervisor respaldado por un VDS utiliza un equilibrador de carga para proporcionar conectividad a los usuarios de desarrollo y operaciones, y a los servicios externos. Puede utilizar el NSX Advanced Load Balancer o el equilibrador de carga de HAProxy.

Para obtener más información, consulte Instalar y configurar NSX Advanced Load Balancer e Instalar y configurar el equilibrador de carga de HAProxy.

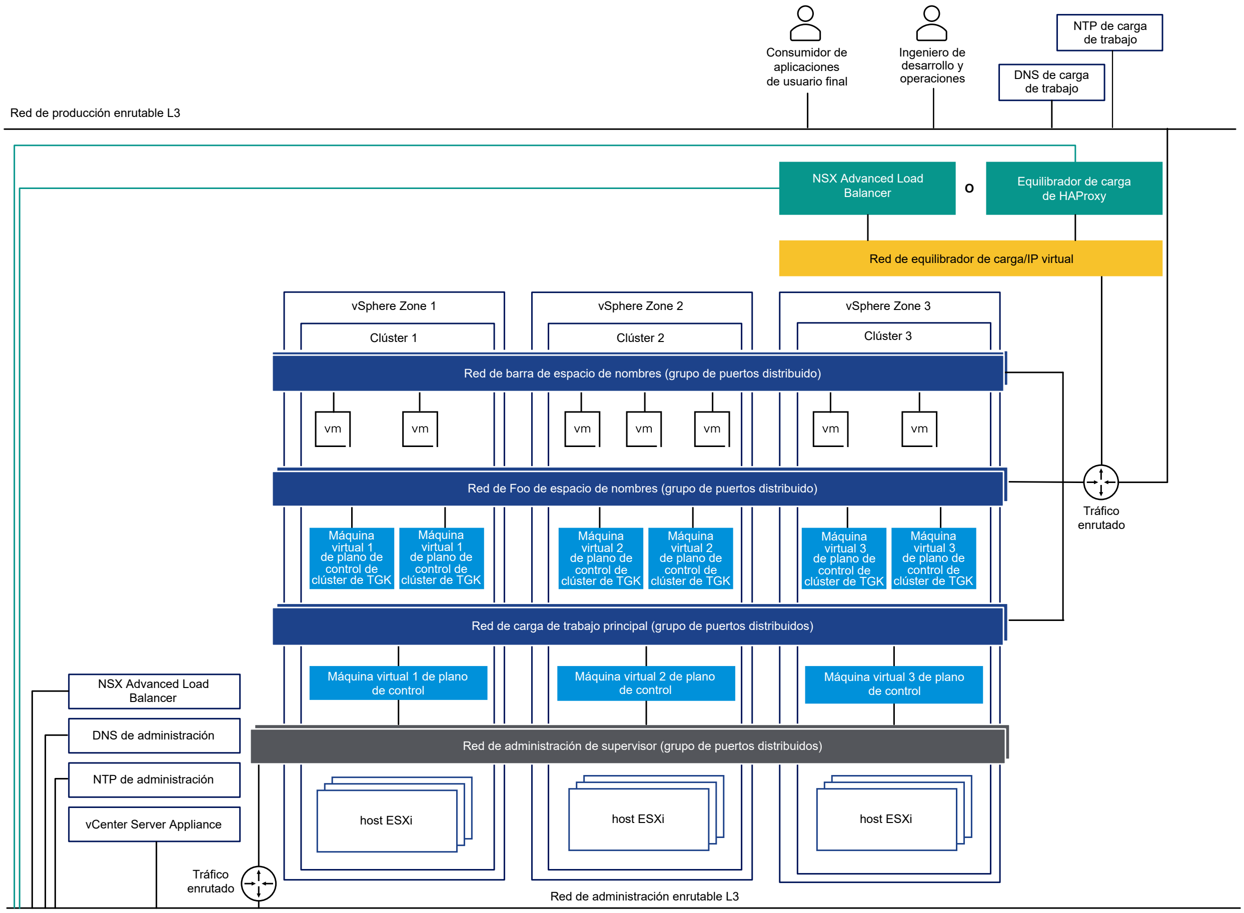
En una configuración de Supervisor de clúster único, el Supervisor está respaldado por un solo clúster de vSphere. Todos los hosts del clúster deben estar conectados a un VDS.

Figura 4-1. Redes de un Supervisor de clúster único con VDS



En un Supervisor de tres zonas, se implementa el Supervisor en tres zonas de vSphere, cada una asignada a un clúster de vSphere. Todos los hosts de estos clústeres de vSphere deben estar conectados al mismo VDS. Todos los servidores físicos deben estar conectados a un dispositivo de capa 2. Las redes de carga de trabajo que se configuran en el espacio de nombres abarcan las tres zonas de vSphere.

Figura 4-2. Redes de un Supervisor de tres zonas con VDS



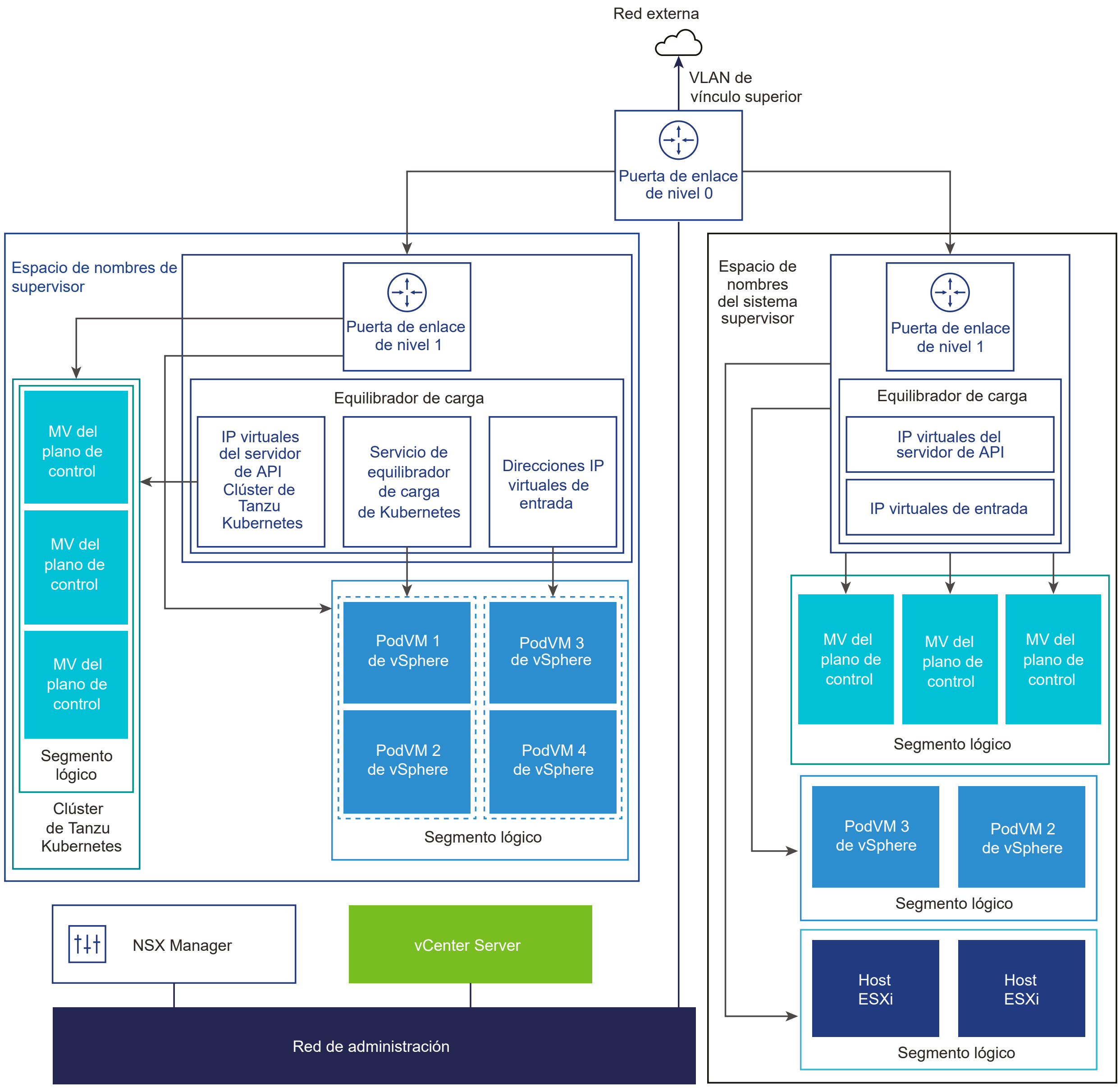
Redes de Supervisor con NSX

NSX proporciona conectividad de red a los objetos dentro de Supervisor y las redes externas. La conectividad con los hosts ESXi que componen el clúster se gestiona mediante las redes vSphere estándar.

También puede configurar manualmente las redes de Supervisor mediante una implementación de NSX existente o mediante la implementación de una nueva instancia de NSX.

Para obtener más información, consulte Instalar y configurar NSX para vSphere IaaS control plane.

Figura 4-3. Redes de Supervisor con NSX



- NSX Container Plugin (NCP) proporciona integración entre NSX y Kubernetes. El componente principal de NCP se ejecuta en un contenedor y se comunica con NSX Manager y con el plano de control de Kubernetes. NCP supervisa los cambios en los contenedores y otros recursos, y administra los recursos de redes, como los puertos lógicos, los segmentos, los enrutadores y los grupos de seguridad de los contenedores mediante una llamada a NSX API.

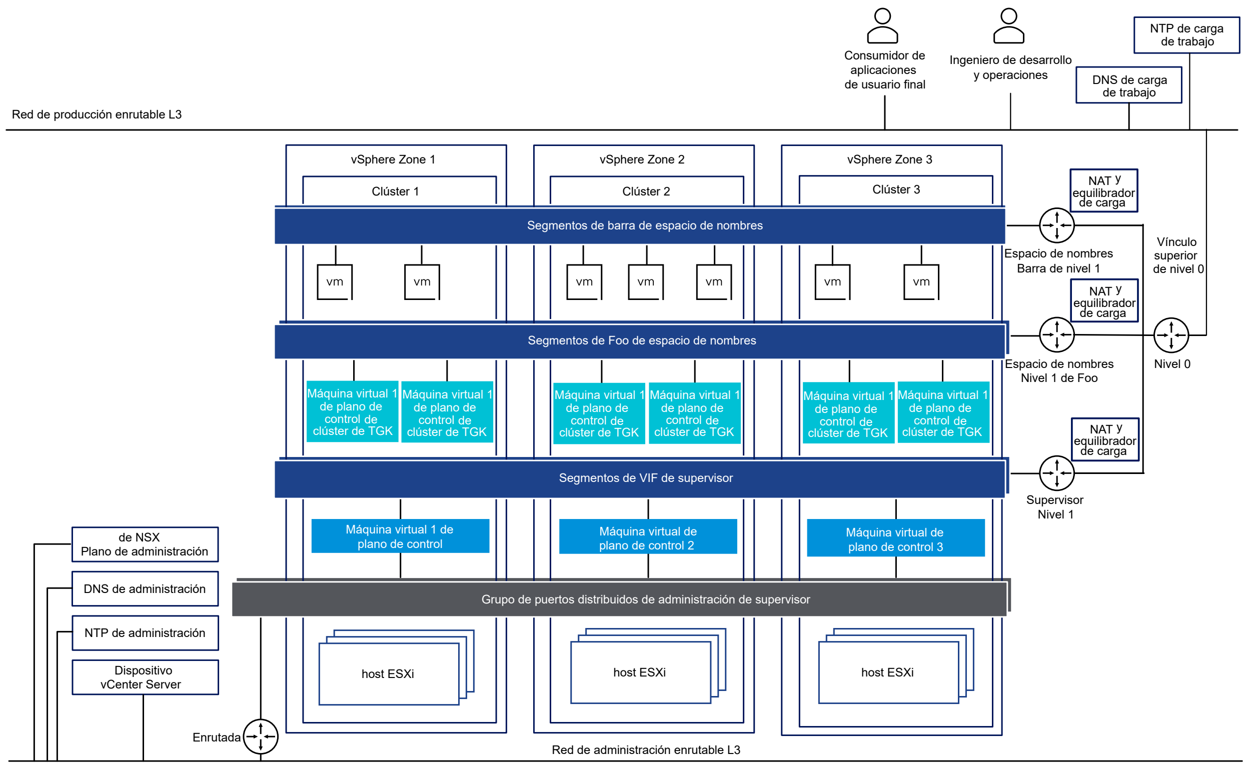
  NCP crea de forma predeterminada una puerta de enlace de nivel 1 compartida para los espacios de nombres del sistema y una puerta de enlace de nivel 1 y un equilibrador de carga para cada espacio de nombres. La puerta de enlace de nivel 1 está conectada a la puerta de enlace de nivel 0 y a un segmento predeterminado.

Los espacios de nombres del sistema son espacios de nombres utilizados por los componentes principales que son esenciales para el funcionamiento de los clústeres de Supervisor y de Tanzu Kubernetes Grid. Los recursos de red compartidos que incluyen la puerta de enlace de nivel 1, el equilibrador de carga y la IP de SNAT se agrupan en un espacio de nombres del sistema.

- NSX Edge proporciona conectividad de redes externas a objetos del Supervisor. El clúster de NSX Edge tiene un equilibrador de carga que proporciona redundancia a los servidores de API de Kubernetes que residen en las máquinas virtuales del plano de control del Supervisor, así como en cualquier aplicación que deba publicarse y a la que se pueda acceder desde fuera del Supervisor.
- Se asocia una puerta de enlace de nivel 0 al clúster de NSX Edge para proporcionar enrutamiento a la red externa. La interfaz de vínculo superior utiliza el protocolo de enrutamiento dinámico, BGP o enrutamiento estático.
- Cada espacio de nombres de vSphere tiene una red independiente y un conjunto de recursos de red compartidos por las aplicaciones que están dentro del espacio de nombres, como la puerta de enlace de nivel 1, el servicio de equilibrador de carga y la dirección IP de SNAT.
- Las cargas de trabajo que se ejecutan en pods de vSphere, máquinas virtuales normales o clústeres de Tanzu Kubernetes Grid, los cuales están en el mismo espacio de nombres, comparten una misma IP de SNAT para la conectividad de norte a sur.
- Las cargas de trabajo que se ejecutan en clústeres de pods de vSphere o Tanzu Kubernetes Grid tendrán la misma regla de aislamiento que implementa el firewall predeterminado.
- No se requiere una IP de SNAT independiente para cada espacio de nombres de Kubernetes. La conectividad de este a oeste entre espacios de nombres no será SNAT.
- Los segmentos de cada espacio de nombres residen en la instancia de VDS que funciona en el modo estándar y está asociada con el clúster de NSX Edge. El segmento proporciona una red de superposición al Supervisor.
- Los Supervisores tienen segmentos separados dentro de la puerta de enlace de nivel 1 compartida. Para cada clúster de Tanzu Kubernetes Grid, los segmentos se definen en la puerta de enlace de nivel 1 del espacio de nombres.
- Los procesos de Spherelet en cada host ESXi se comunican con vCenter Server a través de una interfaz de la red de administración.

En un Supervisor de tres zonas configurado con NSX como pila de redes, todos los hosts de los tres clústeres de vSphere asignados a las zonas deben estar conectados al mismo VDS y participar en la misma zona de transporte superpuesta de NSX. Todos los hosts deben estar conectados al mismo dispositivo físico de capa 2.

Figura 4-4. Redes de un Supervisor de tres zonas con NSX



Redes de Supervisor con NSX y NSX Advanced Load Balancer

NSX proporciona conectividad de red a los objetos dentro de Supervisor y las redes externas. Un Supervisor que esté configurado con NSX puede utilizar NSX Edge o NSX Advanced Load Balancer.

Los componentes de NSX Advanced Load Balancer incluyen el clúster de la NSX Advanced Load Balancer Controller, las máquinas virtuales de los motores de servicio (plano de datos) y el operador de AVI Kubernetes (AKO).

La NSX Advanced Load Balancer Controller interactúa con vCenter Server para automatizar el equilibrio de carga de los clústeres de Tanzu Kubernetes Grid. Se encarga de aprovisionar los motores de servicio, coordinar los recursos entre los motores de servicio y agregar métricas y registros de los motores de servicio. La controladora proporciona una interfaz web, una interfaz de línea de comandos y una API para el funcionamiento del usuario y la integración programática. Después de implementar y configurar la máquina virtual de la controladora, puede implementar un clúster de la controladora para configurar el clúster del plano de control para HA.

El motor de servicio es la máquina virtual del plano de datos. Un motor de servicio ejecuta uno o varios servicios virtuales. La NSX Advanced Load Balancer Controller administra un motor de servicio. La controladora aprovisiona los motores de servicio para alojar servicios virtuales.

El motor de servicio tiene dos tipos de interfaces de red:

- La primera interfaz de red, `vnic0` de la máquina virtual, se conecta a la red de administración, donde puede conectarse a la NSX Advanced Load Balancer Controller.

- Las restantes interfaces, `vnic1 - 8`, se conectan a la red de datos en la que se ejecutan los servicios virtuales.

Las interfaces del motor de servicio se conectan automáticamente a los grupos de puertos de vDS correctos. Cada motor de servicio puede admitir hasta 1000 servicios virtuales.

Un servicio virtual proporciona servicios de equilibrio de carga de capa 4 y capa 7 para cargas de trabajo del clúster de Tanzu Kubernetes Grid. Un servicio virtual se configura con una IP virtual y varios puertos. Cuando se implementa un servicio virtual, el controlador selecciona automáticamente una instancia de ESX Server, aumenta la velocidad de giro de un motor de servicio y lo conecta a las redes correctas (grupos de puertos).

El primer motor de servicio solo se crea después de configurar el primer servicio virtual. Todos los servicios virtuales que se configuren posteriormente utilizarán el motor de servicio existente.

Cada servidor virtual expone un equilibrador de carga de capa 4 con una dirección IP distinta del tipo equilibrador de carga para un clúster de Tanzu Kubernetes Grid. La dirección IP asignada a cada servidor virtual se selecciona en el bloque de direcciones IP otorgado a la controladora cuando se configura.

El operador de AVI Kubernetes (AKO) consulta los recursos de Kubernetes y se comunica con la NSX Advanced Load Balancer Controller para solicitar los recursos de equilibrio de carga correspondientes. El operador de AVI Kubernetes se instala en los Supervisores como parte del proceso de habilitación.

Para obtener más información, consulte Instalar y configurar NSX y NSX Advanced Load Balancer.

Figura 4-5. Redes de Supervisor con NSX y NSX Advanced Load Balancer Controller

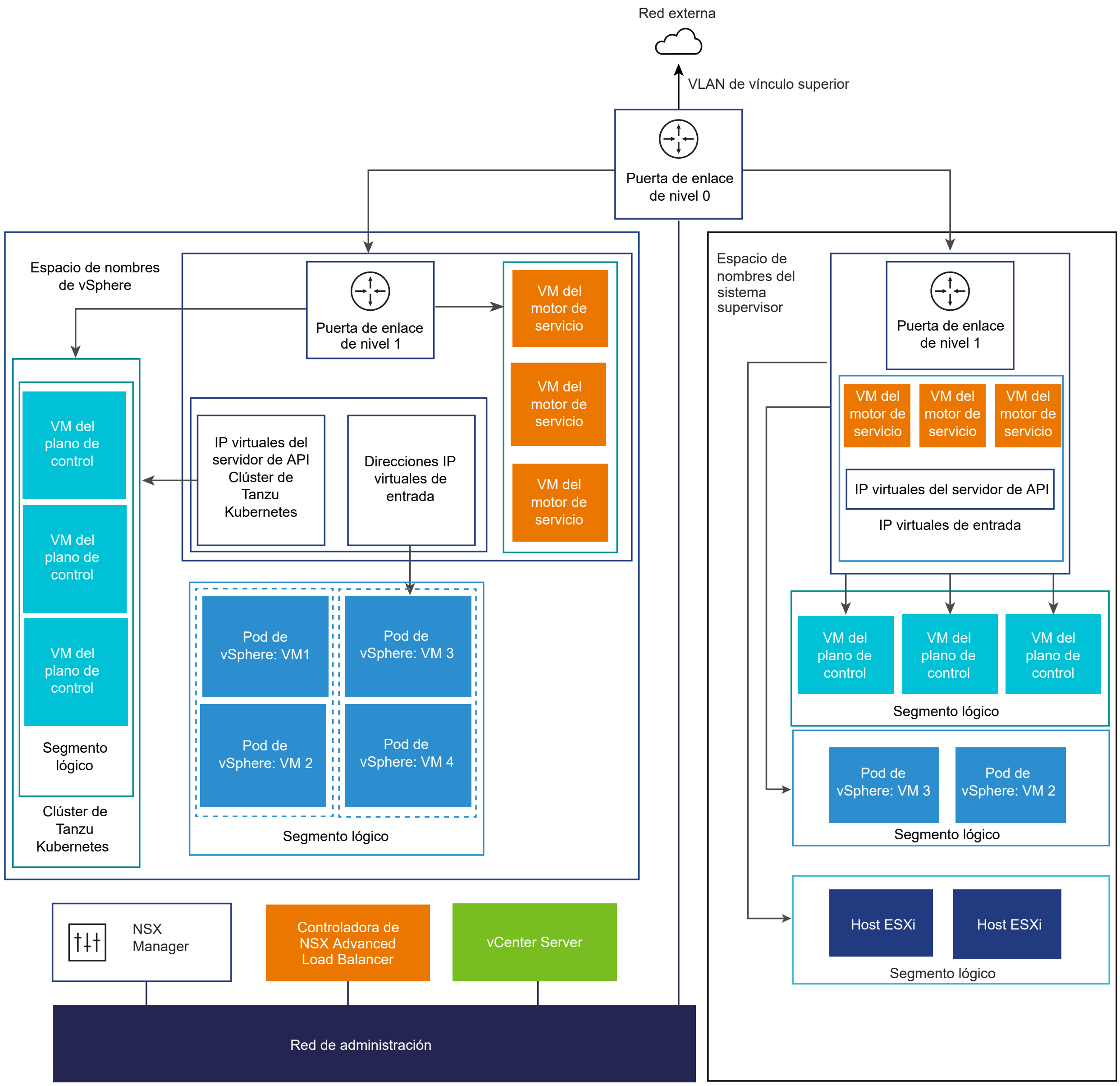
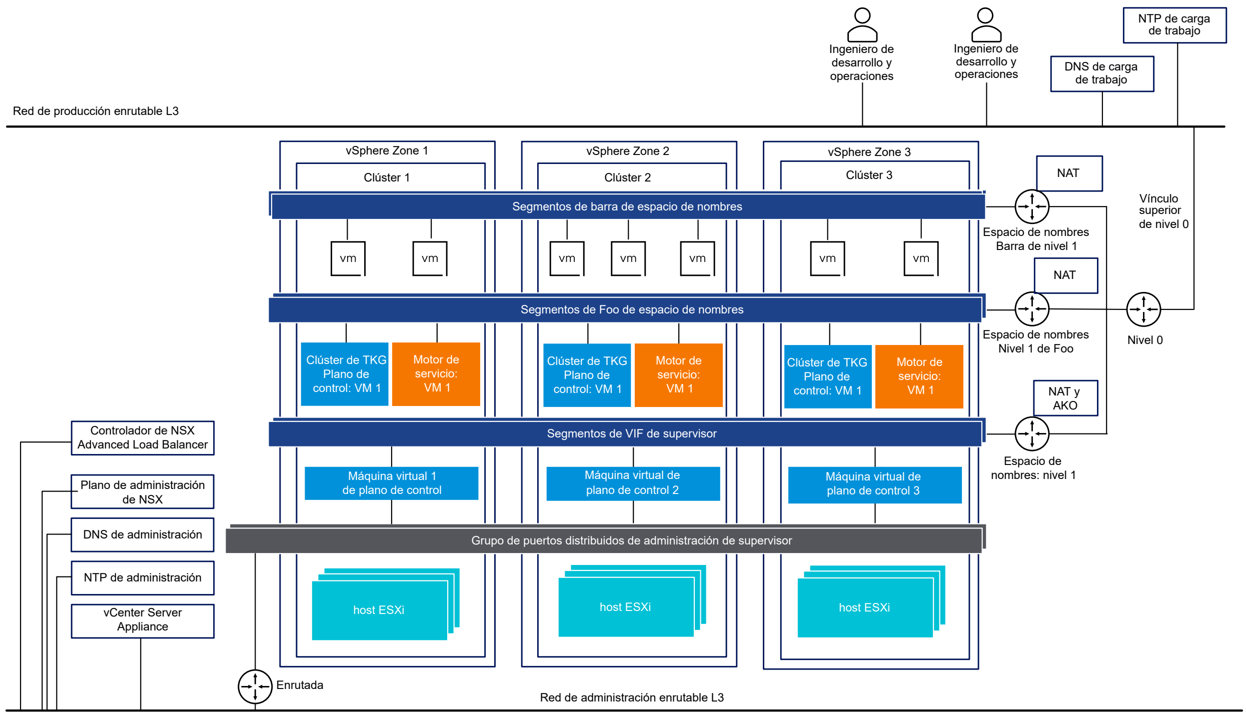


Figura 4-6. Redes de un Supervisor de tres zonas con NSX y NSX Advanced Load Balancer Controller



Importante Cuando configure la NSX Advanced Load Balancer Controller en una implementación de NSX, tenga en cuenta las siguientes consideraciones:

- No se puede implementar la NSX Advanced Load Balancer Controller en una implementación de Enhanced Linked Mode de vCenter Server. Solo se puede implementar la NSX Advanced Load Balancer Controller en una única implementación de vCenter Server. Si hay más de una instancia de vCenter Server vinculada, solo se puede utilizar una de ellas al configurar la NSX Advanced Load Balancer Controller.
- No se puede configurar la NSX Advanced Load Balancer Controller en una topología de nivel 0 de varios niveles. Si el entorno de NSX está configurado con una topología de nivel 0 de varios niveles, solo se puede utilizar una puerta de enlace de nivel 0 mientras configura la NSX Advanced Load Balancer Controller.

Métodos de configuración de redes con NSX

El Supervisor usa una configuración de redes taxativa. Existen dos métodos para configurar las redes del Supervisor con NSX que dan como resultado la implementación del mismo modelo de redes para un Supervisor de una zona:

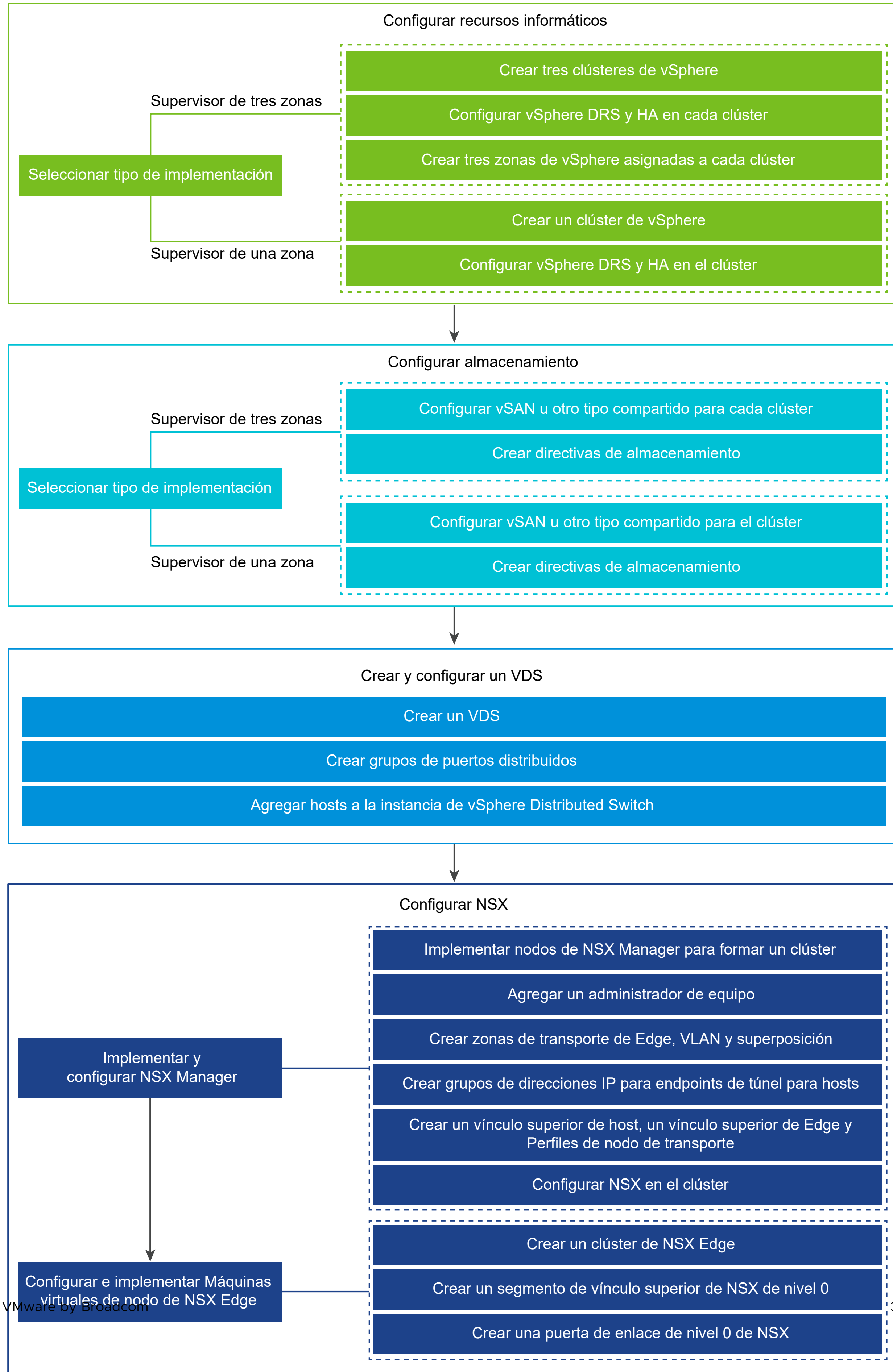
- La forma más sencilla de configurar las redes de Supervisor es mediante VMware Cloud Foundation SDDC Manager. Para obtener más información, consulte la documentación de VMware Cloud Foundation SDDC Manager. Para obtener más información, consulte Guía de administración de VMware Cloud Foundation.

- También puede configurar manualmente las redes de Supervisor mediante una implementación de NSX existente o mediante la implementación de una nueva instancia de NSX. Para obtener más información, consulte Instalar y configurar NSX para vSphere IaaS control plane.

Instalar y configurar NSX para vSphere IaaS control plane

vSphere IaaS control plane requiere una configuración de redes específica para habilitar la conectividad con los Supervisores y los espacios de nombres de vSphere, así como con todos los objetos que se ejecutan en los espacios de nombres, como los pods de vSphere, las máquinas virtuales y los clústeres de Tanzu Kubernetes. Como administrador de vSphere, instale y configure el NSX para vSphere IaaS control plane.

Figura 4-7. Flujo de trabajo para configurar un supervisor con NSX



En esta sección se describe cómo configurar las redes de Supervisor mediante la implementación de una nueva instancia de NSX, pero los procedimientos se aplican también a una implementación de NSX existente. En esta sección también se proporciona información general para comprender cómo actúa VMware Cloud Foundation SDDC Manager cuando configura el dominio de carga de trabajo de Supervisor.

Requisitos previos

- Compruebe que el entorno cumpla con los requisitos del sistema para configurar un clúster de vSphere como un Supervisor. Para obtener información sobre los requisitos, consulte Requisitos para un supervisor zonal con NSX y Requisitos para la implementación de clúster supervisor con NSX en *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Asigne una licencia de edición de Tanzu al Supervisor.
- Cree directivas de almacenamiento para la colocación de las máquinas virtuales del plano de control, los discos efímeros del pod y las imágenes del contenedor.
- Configure el almacenamiento compartido para el clúster. Se requiere almacenamiento compartido para vSphere DRS, HA y el almacenamiento de volúmenes persistentes de contenedores.
- Compruebe que DRS y HA estén habilitados en el clúster de vSphere y que DRS esté en el modo totalmente automatizado.
- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

Procedimiento

1 Crear y configurar un conmutador distribuido de vSphere

  Para controlar la configuración de redes de todos los hosts en el Supervisor, cree un conmutador vSphere Distributed Switch, cree grupos de puertos distribuidos y asocie los hosts al conmutador.

2 Implementar y configurar el NSX Manager

  Puede usar la instancia de vSphere Client para implementar NSX Manager en el clúster de vSphere y utilizarlo con vSphere IaaS control plane.

3 Crear zonas de transporte

  Las zonas de transporte indican los hosts y las máquinas virtuales que pueden utilizar una red determinada. Una zona de transporte puede abarcar uno o varios clústeres de host.

4 Configurar e implementar un nodo de transporte de NSX Edge

  Puede agregar una máquina virtual de NSX Edge al tejido de NSX y proceder a configurarla como una máquina virtual de nodo de transporte de NSX Edge.

Crear y configurar un conmutador distribuido de vSphere

Para controlar la configuración de redes de todos los hosts en el Supervisor, cree un conmutador vSphere Distributed Switch, cree grupos de puertos distribuidos y asocie los hosts al conmutador.

Procedimiento

1 En vSphere Client, desplácese hasta un centro de datos.

2 En el navegador, haga clic con el botón derecho en el centro de datos y seleccione **Conmutador distribuido > Nuevo conmutador distribuido**.

3 Introduzca un nombre para el nuevo conmutador distribuido.

   Por ejemplo, `DSwitch`.

4 En **Seleccionar versión**, introduzca una versión para el conmutador distribuido.

   Seleccione **8,0**.

5 En **Configurar parámetros**, introduzca la cantidad de puertos de vínculo superior.

   Introduzca un valor de `2`.

6 Revise la configuración y haga clic en **Finalizar**.

7 Haga clic con el botón derecho en el conmutador distribuido que ha creado y seleccione **Configuración > Editar configuración**.

8 En la pestaña **Avanzado**, introduzca un valor superior a 1700 como valor de MTU (bytes) y haga clic en **Aceptar**.

   El tamaño de MTU debe ser 1700 o superior en cualquier red que transporte tráfico superpuesto.

   Por ejemplo, `9000`.

   NSX toma el valor de MTU predeterminado global de 1700.

Crear grupos de puertos distribuidos

Cree grupos de puertos distribuidos para cada vínculo superior del nodo de NSX Edge, TEP de nodo de Edge, red de administración y almacenamiento compartido.

El grupo de puertos predeterminado y los vínculos superiores predeterminados se crean al crear el vSphere Distributed Switch. Debe crear el grupo de puertos de administración, vSAN grupo de puertos. Grupo de puertos de TEP de Edge y NSX Edge grupo de puertos de vínculo superior.

Requisitos previos

Compruebe que se haya creado una instancia de vSphere Distributed Switch.

Procedimiento

1 En vSphere Client, desplácese hasta un centro de datos.

2 En el navegador, haga clic con el botón derecho en el conmutador distribuido y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

3 Cree un grupo de puertos para el vínculo superior de NSX Edge.

   Por ejemplo, `DPortGroup-EDGE-UPLINK`.

4 Configure **Tipo de VLAN** como enlace troncal de VLAN.

5 Acepte el rango troncal de VLAN predeterminado **(0-4094)** .

6 Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

7 Haga clic con el botón derecho en el conmutador distribuido y en el menú **Acciones**, seleccione **Grupo de puertos distribuidos > Administrar grupo de puertos distribuidos**.

8 Seleccione **Formación de equipos y conmutación por error** y haga clic en **Siguiente**.

9 Configure vínculos superiores activos y en espera.

   Por ejemplo, el vínculo superior es `Uplink1` y el vínculo superior en espera es `Uplink2`.

10 Haga clic en **Aceptar** para completar la configuración del grupos de puertos.

11 Repita los pasos del 2 al 10 para crear grupos de puertos para el TEP del nodo de Edge, la red de administración y el almacenamiento compartido.

   Por ejemplo, cree los siguientes grupos de puertos:

Grupo de puertos	Nombre	tipo de VLAN
TEP de nodo de Edge	`DPortGroup-EDGE-TEP`	Configure **Tipo de VLAN** como enlace troncal de VLAN. Configure el vínculo superior activo como `Uplink2` y el vínculo superior en espera como `Uplink1`. **Nota** La VLAN que se utiliza para el TEP de nodos de Edge debe ser diferente de la VLAN utilizada para el TEP de ESXi.
Administración	`DPortGroup-MGMT`	Configure **Tipo de VLAN** como VLAN e introduzca el identificador de VLAN de la red de administración. Por ejemplo, `1060`.
Almacenamiento compartido o vSAN	`DPortGroup-VSAN`	Configure **Tipo de VLAN** como VLAN e introduzca el identificador de VLAN. Por ejemplo, `3082`.

12 Cree grupos de puertos para los siguientes componentes:

- **vSphere vMotion**. Este grupo de puertos es obligatorio para las actualizaciones de Supervisor. Configure el grupo de puertos predeterminado para vMotion.
- **Tráfico de máquina virtual**. Configure el grupo de puertos predeterminado para controlar el tráfico de la máquina virtual.

Agregar hosts a la instancia de vSphere Distributed Switch

Para administrar las redes de su entorno mediante vSphere Distributed Switch, debe asociar los hosts del Supervisor con el conmutador. Para ello, conecte las NIC físicas, los adaptadores de VMkernel y los adaptadores de red de las máquinas virtuales de los hosts al conmutador distribuido.

Requisitos previos

- Compruebe que haya suficientes vínculos superiores disponibles en el conmutador distribuido para asignarles las NIC físicas que desea conectar al conmutador.
- Compruebe que haya al menos un grupo de puertos distribuidos disponible en el conmutador distribuido.
- Compruebe que el grupo de puertos distribuidos tenga configurados vínculos superiores activos en su directiva de formación de equipos y conmutación por error.

Procedimiento

1. En vSphere Client, seleccione **Redes** y desplácese al conmutador distribuido.
2. En el menú **Acciones**, seleccione **Agregar y administrar hosts**.
3. En la página **Seleccionar tarea**, seleccione **Agregar hosts** y haga clic en **Siguiente**.
4. En la página **Seleccionar hosts**, haga clic en **Nuevos hosts**, seleccione los hosts del centro de datos, haga clic en **Aceptar** y, a continuación, haga clic en **Siguiente**.
5. En la página **Administrar adaptadores físicos**, configure las NIC físicas en el conmutador distribuido.
   a. En la lista **En otros conmutadores/sin reclamar**, seleccione una NIC física.

      Si selecciona NIC físicas que ya están conectadas a otros conmutadores, estas se migrarán al conmutador distribuido actual.
   b. Haga clic en **Asignar vínculo superior**.
   c. Seleccione un vínculo superior.
   d. Para asignar el vínculo superior a todos los hosts del clúster, seleccione **Aplicar esta asignación de vínculo superior al resto de los hosts**.
   e. Haga clic en **Aceptar**.

   Por ejemplo, asigne `Uplink 1` a `vmnic0` y `Uplink 2` a `vmnic1`.
6. Haga clic en **Siguiente**.
7. En la página **Administrar adaptadores de VMkernel**, configure los adaptadores de VMkernel.
   a. Seleccione un adaptador VMkernel y haga clic en **Asignar grupo de puertos**.
   b. Seleccione un grupo de puertos distribuidos.

      Por ejemplo, **DPortGroup**.

c Para aplicar el grupo de puertos a todos los hosts del clúster, seleccione **Aplicar esta asignación de grupo de puertos al resto de los hosts**.

d Haga clic en **Aceptar**.

8 Haga clic en **Siguiente**.

9 (opcional) En la página **Migrar redes de máquina virtual**, active la casilla **Migrar redes de máquinas virtuales** para configurar las redes de máquinas virtuales.

a Para conectar todos los adaptadores de red de una máquina virtual a un grupo de puertos distribuido, seleccione la máquina virtual o seleccione un adaptador de red individual para conectar solamente el adaptador.

b Haga clic en **Asignar grupo de puertos**.

c Seleccione un grupo de puertos distribuidos de la lista y haga clic en **Aceptar**.

d Haga clic en **Siguiente**.

Pasos siguientes

Implemente y configure el NSX Manager. Consulte Implementar y configurar el NSX Manager

Implementar y configurar el NSX Manager

Puede usar la instancia de vSphere Client para implementar NSX Manager en el clúster de vSphere y utilizarlo con vSphere IaaS control plane.

Para implementar la instancia de NSX Manager con el archivo OVA, realice los pasos de este procedimiento.

Para obtener información sobre la implementación de NSX Manager a través de la interfaz de usuario o la CLI, consulte la *Guía de instalación de NSX*.

Requisitos previos

- Compruebe que el entorno cumpla con los requisitos de red. Para obtener información sobre los requisitos, consulte Requisitos para un supervisor de tres zonas con NSX Advanced Load Balancer y Requisitos para habilitar un supervisor de clúster único con NSX Advanced Load Balancer en *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Compruebe que los puertos necesarios estén abiertos. Para obtener información sobre los puertos y los protocolos, consulte la *Guía de instalación de NSX*.

Procedimiento

1 Busque el archivo OVA de NSX en el portal de descargas de VMware.

Copie la URL de descarga o descargue el archivo OVA.

2 Haga clic con el botón secundario del ratón y seleccione **Implementar plantilla de OVF** para iniciar el Asistente de instalación.

3. En la pestaña **Seleccione una plantilla de archivo OVF**, introduzca la URL de descarga de OVA o desplácese hasta el archivo OVA.
4. En la pestaña **Seleccionar un nombre y una carpeta**, escriba un nombre para la máquina virtual de NSX Manager.
5. En la pestaña **Seleccionar un recurso informático**, seleccione el clúster de vSphere en el que se implementará NSX Manager.
6. Haga clic en **Siguiente** para revisar los detalles.
7. En la pestaña **Configuración**, seleccione el tamaño de implementación de NSX.

   El tamaño de implementación mínimo recomendado es Medio.
8. En la pestaña **Seleccionar almacenamiento**, seleccione el almacenamiento compartido para la implementación.
9. Para habilitar el aprovisionamiento fino, seleccione **Aprovisionamiento fino** en **Seleccionar formato de disco virtual**.

   Los discos virtuales cuentan con aprovisionamiento grueso de forma predeterminada.
10. En la pestaña **Seleccionar redes**, seleccione el grupo de puertos de administración o la red de destino para NSX Manager en **Red de destino**.

    Por ejemplo, `DPortGroup-MGMT`.
11. En la pestaña **Personalizar plantilla**, introduzca la raíz del sistema, el administrador de la CLI y las contraseñas de auditoría de NSX Manager. Las contraseñas deben cumplir con las restricciones de seguridad para contraseñas.

    - Al menos 12 caracteres.
    - Al menos una letra en minúsculas.
    - Al menos una letra en mayúsculas.
    - Al menos un dígito.
    - Al menos un carácter especial.
    - Al menos cinco caracteres diferentes.
    - El módulo PAM de Linux aplica las reglas de complejidad de contraseña predeterminadas.
12. Introduzca la puerta de enlace IPv4 predeterminada, la red de administración IPv4, la máscara de red de la red de administración, el servidor DNS, la lista de búsqueda de dominios y la dirección IP de NTP.
13. Habilite SSH y permita el inicio de sesión SSH raíz en la línea de comandos de NSX Manager.

    De forma predeterminada, las opciones SSH están deshabilitadas por motivos de seguridad.
14. Compruebe que la especificación de la plantilla de OVF personalizada sea correcta y haga clic en **Finalizar** para iniciar la instalación.

15 Después de que arranque NSX Manager, inicie sesión en la CLI como administrador y ejecute el comando `get interface eth0` para comprobar que la dirección IP se aplicó según lo previsto.

16 Introduzca el comando `get services` para comprobar que se están ejecutando todos los servicios.

Implementar nodos de NSX Manager para formar un clúster

Un clúster de NSX Manager proporciona alta disponibilidad. Los nodos de NSX Manager solo se pueden implementar mediante la interfaz de usuario en los hosts ESXi que administra vCenter Server. Para crear un clúster de NSX Manager, implemente dos nodos adicionales con la finalidad de formar un clúster de tres nodos en total. Cuando se implementa un nodo nuevo desde la interfaz de usuario, este se conecta al primer nodo implementado para formar un clúster. Todos los detalles del repositorio y la contraseña del primer nodo implementado se sincronizan con el nodo que se acaba de implementar.

Requisitos previos

- Compruebe que se haya instalado un nodo de NSX Manager.
- Compruebe que se haya configurado un administrador de equipo.
- Compruebe que los puertos necesarios estén abiertos.
- Compruebe que se haya configurado un almacén de datos en el host ESXi.
- Compruebe que tenga la dirección IP y la puerta de enlace, las direcciones IP del servidor DNS, la lista de búsqueda de dominios y la dirección IP del servidor NTP que utilizará NSX Manager.
- Compruebe que tenga una red de grupos de puertos de máquina virtual de destino. Coloque los dispositivos de NSX en una red de máquinas virtuales de administración.

Procedimiento

1 Desde un explorador, inicie sesión con privilegios de administrador en NSX Manager en https://<manager-ip-address>.

2 Para implementar un dispositivo, seleccione **Sistema > Dispositivos > Agregar NSX Appliance**.

3 Introduzca los detalles del dispositivo.

Opción	Descripción
Nombre de host	Introduzca el nombre del host o el FQDN que se utilizará para el nodo.
Dirección IP/máscara de red de administración	Introduzca una dirección IP que se asignará al nodo.
Puerta de enlace de administración	Introduzca una dirección IP de puerta de enlace que vaya a utilizar el nodo.
Servidores DNS	Introduzca la lista de direcciones IP del servidor DNS que vaya a utilizar el nodo.

Opción	Descripción
Servidor NTP	Introduzca la lista de direcciones IP del servidor NTP.
Tamaño del nodo	Seleccione el formato **Mediano (6 vCPU, 24 GB de RAM, 300 GB de almacenamiento)** en las opciones.

4 Introduzca los detalles de configuración del dispositivo.

Opción	Descripción
Administrador de equipo	Seleccione la instancia de vCenter Server que configuró como administrador de equipo.
Clúster de proceso	Seleccione el clúster al que se debe unir el nodo.
Almacén de datos	Seleccione un almacén de datos para los archivos de nodo.
Formato de disco virtual	Seleccione el formato **Aprovisionamiento fino**.
Red	Haga clic en **Seleccionar red** para seleccionar la red de administración del nodo.

5 Introduzca los detalles de acceso y las credenciales.

Opción	Descripción
Habilitar SSH	Active el botón para permitir el inicio de sesión SSH en el nodo nuevo.
Habilitar el acceso raíz	Active el botón para permitir el acceso raíz en el nodo nuevo.
Credenciales raíz del sistema	Establezca la contraseña raíz y confírmela para el nodo nuevo. La contraseña debe cumplir las restricciones de seguridad para contraseñas. ■ Al menos 12 caracteres. ■ Al menos una letra en minúsculas. ■ Al menos una letra en mayúsculas. ■ Al menos un dígito. ■ Al menos un carácter especial. ■ Al menos cinco caracteres diferentes. ■ El módulo PAM de Linux aplica las reglas de complejidad de contraseña predeterminadas.
Credenciales de la CLI de administración y credenciales de la CLI de auditoría	Seleccione la casilla de verificación **Igual que la contraseña raíz** si desea usar la misma contraseña que configuró para la raíz; de lo contrario, anule la selección de esta casilla y establezca otra contraseña diferente.

6 Haga clic en **Instalar dispositivo**.

Se implementará el nodo nuevo. Puede realizar un seguimiento del proceso de implementación en la página **Sistema> > Dispositivos**. No agregue más nodos hasta que finalice la instalación y el clúster esté estable.

7 Espere a que finalice la implementación, la creación del clúster y la sincronización del repositorio.

   El proceso de unión y estabilización del clúster puede tardar entre 10 y 15 minutos. Compruebe que el estado de cada grupo de servicios del clúster sea `ACTIVO` antes de realizar cualquier otro cambio en el clúster.

8 Después de que arranque el nodo, inicie sesión en la CLI como administrador y ejecute el comando `get interface eth0` para comprobar que la dirección IP se aplicó según lo previsto.

9 Si el clúster solo tiene dos nodos, agregue otro dispositivo. Seleccione **Sistema > Dispositivos > Agregar NSX Appliance** y repita los pasos de configuración.

Agregar una licencia

Agregue una licencia mediante el NSX Manager.

Requisitos previos

Obtenga una licencia Avanzada o superior de NSX.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Licencias > Agregar**.

3 Introduzca la clave de licencia.

4 Haga clic en **Agregar**.

Agregar un administrador de equipo

Un administrador de equipo es una aplicación que gestiona recursos como hosts y máquinas virtuales. Configure la instancia de vCenter Server que está asociada con la instancia de NSX como administrador de equipo en NSX Manager.

Para obtener más información, consulte la *Guía de administración de NSX*.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Administradores de equipo > Agregar**

3 Introduzca los detalles del administrador de equipo.

Opción	Descripción
Nombre y descripción	Introduzca el nombre y la descripción del vCenter Server.
Tipo	El tipo predeterminado es VMware vCenter.

Opción	Descripción
Varias instancias de NSX	Deje esta opción sin seleccionar. La opción de varias instancias de NSX permite registrar la misma instancia de vCenter Server con varias instancias de NSX Manager. Esta opción no es compatible en los clústeres de Supervisor y vSphere Lifecycle Manager.
FQDN o dirección IP	Introduzca el FQDN o la dirección IP de la instancia del vCenter Server.
Puerto HTTPS del proxy inverso	El puerto predeterminado es 443. Si utiliza otro puerto, compruebe que el puerto esté abierto en todos los dispositivos de NSX Manager. Establezca el puerto de proxy inverso para registrar el administrador de equipos en NSX.
Nombre de usuario y contraseña	Introduzca las credenciales de inicio de sesión de vCenter Server.
Huella digital de SHA-256	Escriba el valor del algoritmo de huella digital SHA-256 de vCenter Server.

Puede mantener los valores predeterminados para los demás ajustes.

Si deja el valor de huella digital en blanco, se le solicitará que acepte la huella digital que proporciona el servidor. Tras aceptar la huella digital, NSX tarda unos segundos en detectar y registrar los recursos de vCenter.

4 Seleccione **Habilitar confianza** para permitir que vCenter Server se comunique con NSX.

5 Si no proporcionó un valor de huella digital para NSX Manager, el sistema identificará la huella digital y la mostrará.

6 Haga clic en **Agregar** para aceptar la huella digital.

Resultados

Después de cierto tiempo, el administrador de equipos se registra en vCenter Server y el estado de la conexión cambia a `Activo`. Si el FQDN o el PNID de vCenter Server cambian, debe volver a registrarlos en NSX Manager. Para obtener más información, consulte Registrar vCenter Server en NSX Manager.

Nota Después de que el vCenter Server se registre correctamente, no apague ni elimine la máquina virtual de NSX Manager sin eliminar primero el administrador de equipo. De lo contrario, cuando implemente un nuevo NSX Manager, no podrá volver a registrar el mismo vCenter Server. Recibirá un error que indica que vCenter Server ya se registró en otra instancia de NSX Manager.

Puede hacer clic en el nombre del administrador de equipo para ver los detalles, editar el administrador de equipo o administrar las etiquetas que se aplican al administrador de equipo.

Crear zonas de transporte

Las zonas de transporte indican los hosts y las máquinas virtuales que pueden utilizar una red determinada. Una zona de transporte puede abarcar uno o varios clústeres de host.

Como administrador de vSphere, utilice las zonas de transporte predeterminadas o cree las siguientes:

- Una zona de transporte superpuesta que utilizan las máquinas virtuales del plano de control del Supervisor.
- Una zona de transporte de VLAN para los nodos de NSX Edge que se utilizará para los vínculos superiores a la red física.

Procedimiento

1. Inicie sesión en NSX Manager.
2. Seleccione **Sistema > Tejido > Zonas de transporte > Agregar**.
3. Introduzca un nombre para la zona de transporte y, opcionalmente, una descripción.
4. Seleccione un tipo de tráfico.

   Puede seleccionar **Superposición** o **VLAN**.

   Las siguientes zonas de transporte existen de forma predeterminada:

   - Una zona de transporte de VLAN con el nombre `nsx-vlan-transportzone`.
   - Una zona de transporte superpuesta con el nombre `nsx-overlay-transportzone`.
5. (opcional) Introduzca uno o varios nombres de directiva de formación de equipos de enlace ascendente.

   Los segmentos asociados a las zonas de transporte usan estas directivas de formación de equipos con nombre. Si los segmentos no encuentran una directiva de formación de equipos con nombre que coincida, se utilizará la directiva de formación de equipos de vínculo superior predeterminada.

Resultados

La nueva zona de transporte aparece en la página **Zonas de transporte**.

Crear un grupo de direcciones IP para las direcciones IP del endpoint de túnel del host

Cree grupos de direcciones IP para los endpoints de túnel del host ESXi (TEP). Los TEP son las direcciones IP de origen y destino que se utilizan en el encabezado IP externo para identificar los hosts ESXi que originan y finalizan la encapsulación NSX de tramas superpuestas. Puede utilizar DHCP o grupos de direcciones IP configuradas manualmente para las direcciones IP de TEP.

Procedimiento

1. Inicie sesión en NSX Manager.
2. Seleccione **Redes > Grupos de direcciones IP > Agregar grupo de direcciones IP**.

3 Introduzca los siguientes detalles del grupo de direcciones IP.

Opción	Descripción
Nombre y descripción	Introduzca el nombre del grupo de direcciones IP y la descripción opcional. Por ejemplo, `ESXI-TEP-IP-POOL`.
Rangos de IP	Introduzca el rango de asignación de IP. Por ejemplo, `192.23.213.158 - 192.23.213.160`
Puerta de enlace	Introduzca la dirección IP de la puerta de enlace. Por ejemplo, `192.23.213.253`.
CIDR	Introduzca la dirección de red en una notación CIDR. Por ejemplo, `192.23.213.0/24`.

4 Haga clic en **Agregar** y **Aplicar**.

Resultados

Compruebe que los grupos de direcciones IP de TEP que creó aparezcan en la página **Grupo de direcciones IP**.

Cree un grupo de direcciones IP para nodos de Edge

Cree grupos de direcciones IP para los nodos de Edge. No es necesario que las direcciones de TEP se puedan enrutar. Puede utilizar cualquier esquema de direcciones IP que permita al TEP de Edge comunicarse con el TEP del host.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Redes > Grupos de direcciones IP > Agregar grupo de direcciones IP**.

3 Introduzca los siguientes detalles del grupo de direcciones IP.

Opción	Descripción
Nombre y descripción	Introduzca el nombre del grupo de direcciones IP y la descripción opcional. Por ejemplo, `EDGE-TEP-IP-POOL`.
Rangos de IP	Introduzca el rango de asignación de IP. Por ejemplo, `192.23.213.1 - 192.23.213.10`.
Puerta de enlace	Introduzca la dirección IP de la puerta de enlace. Por ejemplo, `192.23.213.253`.
CIDR	Introduzca la dirección de red en una notación CIDR. Por ejemplo, `192.23.213.0/24`.

4 Haga clic en **Agregar** y **Aplicar**.

Resultados

Compruebe que los grupos de direcciones IP de que creó aparezcan en la página **Grupo de direcciones IP**.

Crear un perfil de host de vínculo superior

Un perfil de host de vínculo superior define las directivas para los vínculos superiores de los hosts ESXi a los segmentos de NSX.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de vínculo superior > Agregar**.

3 Introduzca un nombre para el perfil de vínculo superior y, si lo desea, una descripción del perfil de vínculo superior.

   Por ejemplo, `ESXI-UPLINK-PROFILE`.

4 En la sección **Formación de equipos**, haga clic en **Agregar** para agregar una directiva de formación de equipos de asignación de nombres y configure una directiva de **Orden de conmutación por error**.

   Se especifica una lista de los vínculos superiores activos y cada interfaz en el nodo de transporte está fijada a un vínculo superior activo. Esta configuración permite el uso de varios vínculos superiores activos al mismo tiempo.

5 Configure vínculos superiores activos y en espera.

   Por ejemplo, configure `uplink-1` como el vínculo superior activo y `uplink-2` como el vínculo superior en espera.

6 Introduzca un valor de VLAN de transporte.

   El endpoint de túnel (Tunnel Endpoint, TEP) utiliza la VLAN de transporte establecida en el tráfico de superposición de etiquetas de perfil de vínculo superior y el identificador de VLAN. Por ejemplo, `1060`.

7 Introduzca el valor de MTU.

   El valor predeterminado de la MTU del perfil de vínculo superior es 1600.

   Nota El valor debe ser al menos 1600, pero no mayor que el valor de MTU en los conmutadores físicos y vSphere Distributed Switch.

Crear un perfil de vínculo superior de Edge

Cree un perfil de vínculo superior con la directiva de formación de equipos de orden de conmutación por error con un vínculo superior activo para el tráfico de superposición de máquinas virtuales de Edge.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de vínculo superior > Agregar**.

3 Introduzca un nombre de perfil de enlace ascendente y, de forma opcional, agregue una descripción de perfil de enlace ascendente.

   Por ejemplo, `EDGE-UPLINK-PROFILE`.

4 En la sección **Formación de equipos**, haga clic en **Agregar** para agregar una directiva de formación de equipos de asignación de nombres y configure una **directiva de conmutación por error**.

   Se enumera una lista de los vínculos superiores activos y cada interfaz en el nodo de transporte está fijada a un vínculo superior activo. Esta configuración permite el uso de varios vínculos superiores activos al mismo tiempo.

5 Configure un vínculo superior activo.

   Por ejemplo, configure `uplink-1` como vínculo superior activo.

6 Consulte los vínculos superiores en la página **Perfil de vínculo superior**.

Crear un perfil de nodo de transporte

Un perfil de nodo de transporte define la forma en que se instala y configura NSX en los hosts de un clúster concreto al que está conectado el perfil.

Requisitos previos

Compruebe que se creó una zona de transporte superpuesta.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de nodo de transporte > Agregar**.

3 Introduzca un nombre para el perfil de nodo de transporte y, opcionalmente, una descripción.

   Por ejemplo, `HOST-TRANSPORT-NODE-PROFILE`.

4 En la sección **Nuevo conmutador de nodo**, seleccione **Tipo** como `VDS`.

5 Seleccione **Modo** como `Standard`.

6 Seleccione vCenter Server y los nombres del conmutador distribuido de la lista.

   Por ejemplo, `DSwitch`

7 Seleccione la zona de transporte superpuesta creada anteriormente.

   Por ejemplo, `NSX-OVERLAY-TRANSPORTZONE`.

8 Seleccione el perfil de host de vínculo superior creado anteriormente.

   Por ejemplo, `ESXI-UPLINK-PROFILE`.

9 Seleccione **Usar grupo de IP** en la lista **Asignación de IP**.

10 Seleccione el grupo de TEP de host creado anteriormente.

   Por ejemplo, `ESXI-TEP-IP-POOL`.

11 En **Asignación de conmutador de directiva de formación de equipos**, haga clic en el icono de edición y asigne los vínculos superiores definidos en el perfil de vínculo superior de NSX a los vínculos superiores de vSphere Distributed Switch.

   Por ejemplo, asigne `uplink-1 (active)` a `Uplink 1` y `uplink-2 (standby)` a `Uplink 2`.

12 Haga clic en **Agregar**.

13 Compruebe que el perfil que creó está incluido en la lista de la página **Perfiles de nodo de transporte**.

Configurar NSX en el clúster

Para instalar NSX y preparar la superposición de TEP, aplique el perfil de nodo de transporte al clúster de vSphere.

Requisitos previos

Compruebe que se creó un perfil de nodo de transporte.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de host**.

3 En el menú desplegable **Administrado por**, seleccione un vCenter Server existente.

   La página muestra los clústeres de vSphere disponibles.

4 Seleccione el clúster de proceso en el que desea configurar NSX.

5 Haga clic en **Configurar NSX**.

6 Seleccione el perfil de nodo de transporte creado previamente y haga clic en **Aplicar**.

   Por ejemplo, `HOST-TRANSPORT-NODE-PROFILE`.

7 En la página **Nodo de transporte de host**, compruebe que el estado de configuración de NSX sea `Success` y que el estado de conectividad de los hosts en el clúster de NSX Manager sea `Up`.

Resultados

El perfil de nodo de transporte creado anteriormente se aplica al clúster de vSphere para instalar NSX y preparar la superposición de los TEP.

Configurar e implementar un nodo de transporte de NSX Edge

Puede agregar una máquina virtual de NSX Edge al tejido de NSX y proceder a configurarla como una máquina virtual de nodo de transporte de NSX Edge.

Requisitos previos

Compruebe que haya creado las zonas de transporte, el perfil de enlace ascendente de Edge y el grupo de direcciones IP de TEP de Edge.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de Edge > Agregar máquina virtual de Edge**.

3 En **Nombre y descripción**, escriba un nombre para NSX Edge.

   Por ejemplo, `nsx-edge-1`

4 Introduzca el nombre de host o FQDN de vCenter Server.

   Por ejemplo, `nsx-edge-1.lab.com`.

5 Seleccione el formato `Large`.

6 En **Credenciales**, introduzca la CLI y las contraseñas raíz de NSX Edge. Las contraseñas deben cumplir con las restricciones de seguridad para contraseñas.

   - Al menos 12 caracteres.
   - Al menos una letra en minúsculas.
   - Al menos una letra en mayúsculas.
   - Al menos un dígito.
   - Al menos un carácter especial.
   - Al menos cinco caracteres diferentes.
   - El módulo PAM de Linux aplica las reglas de complejidad de contraseña predeterminadas.

7 Habilite **Permitir inicio de sesión SSH** para las credenciales raíz y de CLI.

8 En **Configurar implementación**, configure las siguientes propiedades:

Opción	Descripción
Administrador de equipo	Seleccione el administrador de equipo en el menú desplegable. Por ejemplo, seleccione `vCenter`.
Clúster	Seleccione el clúster en el menú desplegable. Por ejemplo, seleccione `Compute-Cluster`.
Almacén de datos	Seleccione el almacén de datos compartido de la lista. Por ejemplo, `vsanDatastore`.

9 Configure los ajustes del nodo.

Opción	Descripción
Asignación de IP	Seleccione Estática. Introduzca los valores de: ■ **IP de administración**: introduzca la dirección IP en la misma VLAN que la red de administración de vCenter Server. Por ejemplo, `10.197.79.146/24`. ■ **Puerta de enlace predeterminada**: la puerta de enlace predeterminada de la red de administración. Por ejemplo, `10.197.79.253`.
Interfaz de administración	Haga clic en **Seleccionar interfaz** y, a continuación, seleccione el grupo de puertos de vSphere Distributed Switch en la misma VLAN de la red de administración en el menú desplegable que creó anteriormente. Por ejemplo, `DPortGroup-MGMT`.

10 En **Configurar NSX**, haga clic en **Agregar conmutador** para configurar las propiedades del conmutador.

11 Utilice el nombre predeterminado para el **Nombre del conmutador de Edge**.

Por ejemplo, `nvds1`.

12 Seleccione la zona de transporte a la que pertenece el nodo de transporte.

Seleccione las zonas de transporte superpuestas creadas anteriormente.

Por ejemplo, `nsx-overlay-transportzone`.

13 Seleccione el perfil de vínculo superior de Edge creado anteriormente.

Por ejemplo, `EDGE-UPLINK-PROFILE`.

14 Seleccione **Usar grupo de IP** en **Asignación de IP**.

15 Seleccione el grupo de IP de TEP de Edge creado anteriormente.

Por ejemplo, `EDGE-TEP-IP-POOL`.

16 En la sección **Asignación de conmutador de directiva de formación de equipos**, asigne el vínculo superior a los perfiles de vínculo superior de Edge creados anteriormente.

Por ejemplo, para `Uplink1`, seleccione `DPortGroup-EDGE-TEP`.

17 Repita los pasos 10 a 16 para agregar un conmutador nuevo.

Por ejemplo, configure los siguientes valores:

Propiedad	Valor
Nombre del conmutador de Edge	`nvds2`
Zona de transporte	`nsx-vlan-transportzone`

Propiedad	Valor
Perfil de vínculo superior de Edge	`EDGE-UPLINK-PROFILE`
Asignación de conmutador de directiva de formación de equipos	`DPortGroup-EDGE-UPLINK`

18 Haga clic en **Finalizar**.

19 Repita los pasos 2 a 18 para una segunda máquina virtual de NSX Edge.

20 Consulte el estado de conexión en la página **Nodos de transporte de Edge**.

Crear un clúster de NSX Edge

Para asegurarse de que al menos un NSX Edge siempre esté disponible, cree un clúster de NSX Edge.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Nodos > Clústeres de Edge > Agregar**.

3 Introduzca el nombre del clúster NSX Edge.

   Por ejemplo, `EDGE-CLUSTER`.

4 Seleccione el perfil de clúster NSX Edge predeterminado en el menú desplegable.

   Seleccione **nsx-default-edge-high-availability-profile**.

5 En el menú desplegable **Tipo de miembro**, seleccione el **nodo de Edge**.

6 En la columna **Disponible**, seleccione las máquinas virtuales de NSX Edge creadas previamente y haga clic en la flecha derecha para moverlas a la columna **Seleccionada**.

7 Por ejemplo, `nsx-edge-1` y `nsx-edge-2`.

8 Haga clic en **Guardar**.

Crear un segmento de vínculo superior de nivel 0

El segmento de vínculo superior de nivel 0 proporciona conectividad de norte a sur desde NSX hasta la infraestructura física.

Requisitos previos

Compruebe que haya creado una puerta de enlace de nivel 0.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Redes > Segmentos > Agregar segmento**.

3 Introduzca un nombre para el segmento.

   Por ejemplo, `TIER-0-LS-UPLINK`.

4 Seleccione la zona de transporte creada previamente.

   Por ejemplo, seleccione `nsx-vlan-transportzone`.

5 Conmute **Estado de administrador** para habilitarlo.

6 Introduzca un identificador de VLAN de la puerta de enlace de nivel 0.

   Por ejemplo, `1089`.

7 Haga clic en **Guardar**.

Crear una puerta de enlace de nivel 0

La puerta de enlace de nivel 0 es el enrutador lógico de NSX que proporciona conectividad de norte a sur para las redes lógicas de NSX a la infraestructura física. vSphere IaaS control plane admite varias puertas de enlace de nivel 0 en distintos clústeres de NSX Edge en la misma zona de transporte.

Una puerta de enlace de nivel 0 tiene conexiones de vínculo inferior con puertas de enlace de nivel 1, y conexiones externas con redes físicas.

Puede configurar el modo de HA (alta disponibilidad) de una puerta de enlace de nivel 0 para que sea activo-activo o activo-en espera. Los siguientes servicios solo se admiten en el modo activo-en espera:

- NAT
- Equilibrio de carga
- Firewall con estado
- VPN

El ARP de proxy se habilita automáticamente en una puerta de enlace de nivel 0 cuando una regla NAT o una VIP de equilibrador de carga utiliza una dirección IP de la subred de la interfaz externa de puerta de enlace de nivel 0. Al habilitar proxy-ARP, los hosts de los segmentos superpuestos y los hosts de un segmento de VLAN pueden intercambiar tráfico de red entre sí sin implementar ningún cambio en el tejido de redes físicas.

Antes de NSX 3.2, el proxy ARP también se admite en una puerta de enlace de nivel 0 en una configuración activa-en espera. A partir de NSX 3.2, el proxy ARP también se admite en una puerta de enlace de nivel 0 en una configuración activa-activa.

Para obtener más información, consulte la *Guía de administración de NSX*.

Requisitos previos

Compruebe que se creó un clúster de NSX Edge.

Procedimiento

1 Inicie sesión en NSX Manager.
2 Seleccione **Redes > Puertas de enlace de nivel 0**.
3 Haga clic en **Agregar puerta de enlace de nivel 0**.
4 Introduzca un nombre para la puerta de enlace de nivel 0.

   Por ejemplo, `Tier-0_VWT`.
5 Seleccione un modo HA activo-en espera.

   En el modo activo-en espera, el miembro activo elegido procesa todo el tráfico. Si se produce un error en el miembro activo, se elige un nuevo miembro para que esté activo.
6 Seleccione el clúster de NSX Edge creado anteriormente.

   Por ejemplo, seleccione `EDGE-CLUSTER`.
7 Haga clic en **Guardar**.

   Se crea la puerta de enlace de nivel 0.
8 Seleccione **Sí** para continuar con la configuración.
9 Configure interfaces.

   a Expanda **Interfaces** y haga clic en **Establezca la opción**.

   b Haga clic en **Agregar interfaz**.

   c Escriba un nombre.

      Por ejemplo, introduzca el nombre `TIER-0_VWT-UPLINK1`.

   d En **Tipo**, seleccione **Externo**.

   e Introduzca una dirección IP del enrutador lógico de Edge – VLAN de vínculo superior. La dirección IP debe ser diferente de la dirección IP de administración configurada para las máquinas virtuales de NSX Edge creadas previamente.

      Por ejemplo, `10.197.154.1/24`.

   f En **Conectado a**, seleccione el segmento de vínculo superior de nivel 0 que creó anteriormente.

      Por ejemplo, `TIER-0-LS-UPLINK`

   g Seleccione un nodo de NSX Edge de la lista.

      Por ejemplo, `nsx-edge-1`.

   h Haga clic en **Guardar**.

i Repita los pasos de "a" a "h" para la segunda interfaz.

Por ejemplo, cree un segundo `TIER-0_VWT-UPLINK2` de vínculo superior con la dirección IP `10.197.154.2/24` conectado al nodo de `nsx-edge-2` Edge.

j Haga clic en **Cerrar.**

10 Para configurar la alta disponibilidad, haga clic en **Establezca la opción** en **Configuración de VIP de alta disponibilidad**.

a Haga clic en **AGREGAR CONFIGURACIÓN DE VIP DE ALTA DISPONIBILIDAD**.

b Introduzca la dirección IP.

Por ejemplo, `10.197.154.3/24`

c Seleccione las interfaces.

Por ejemplo, `TIER-0_WVT-UPLINK1` y `TIER-0_WVT-UPLINK2`.

d Haga clic en **Agregar** y **Aplicar**.

11 Para configurar el enrutamiento, haga clic en **Enrutamiento**.

a Haga clic en **Establecer** en Rutas estáticas.

b Haga clic en **AGREGAR RUTA ESTÁTICA**.

c Escriba un nombre.

Por ejemplo, `DEFAULT-STATIC-ROUTE`.

d Introduzca `0.0.0.0/0` para la dirección IP de red.

e Para configurar los siguientes saltos, haga clic en **Establecer salto siguiente** y, a continuación, en **Agregar salto siguiente**.

f Introduzca la dirección IP del enrutador del siguiente salto. Suele ser la puerta de enlace predeterminada de la VLAN de la red de administración desde la VLAN de vínculo superior del enrutador lógico de NSX Edge.

Por ejemplo, `10.197.154.253`.

g Haga clic en **Agregar**, **Aplicar** y **GUARDAR**.

h Haga clic en **Cerrar**.

12 Para verificar la conectividad, asegúrese de que un dispositivo externo de la arquitectura física pueda hacer ping en los vínculos superiores que configuró.

Pasos siguientes

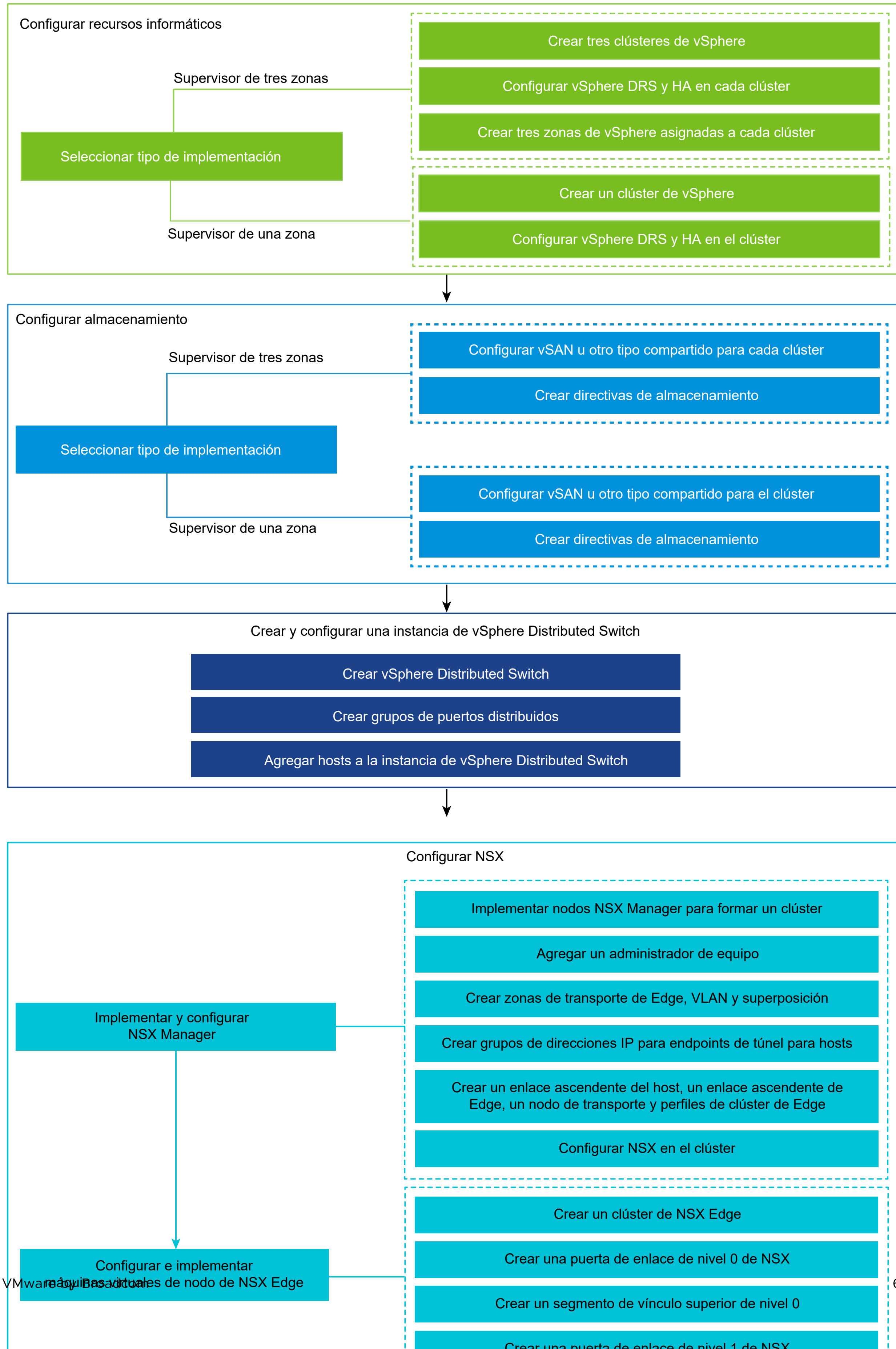
Configure Supervisor. Consulte Implementar un Supervisor de zona única con redes de NSX.

Instalar y configurar NSX y NSX Advanced Load Balancer

En un entorno de Supervisor que utiliza NSX como pila de redes, puede utilizar NSX Advanced Load Balancer para los servicios de equilibrador de carga.

En esta sección, se describe cómo configurar las redes de Supervisor mediante la implementación de instancias nuevas de NSX y NSX Advanced Load Balancer. El procedimiento para instalar y configurar NSX Advanced Load Balancer también se aplica a una implementación de NSX existente.

Figura 4-8. Flujo de trabajo para configurar un supervisor con NSX y NSX Advanced Load Balancer



Crear una instancia de vSphere Distributed Switch para un Supervisor para su uso con NSX Advanced Load Balancer

Para configurar el clúster de vSphere que utiliza la pila de redes de NSX y NSX Advanced Load Balancer como Supervisor, debe crear una instancia de vSphere Distributed Switch. Cree grupos de puertos en el conmutador distribuido que puede configurar como redes de cargas de trabajo en Supervisor. NSX Advanced Load Balancer necesita un grupo de puertos distribuidos para conectar las interfaces de datos del motor de servicio. El grupo de puertos se utiliza para poner las IP virtuales (VIP) de la aplicación en los motores de servicio.

Requisitos previos

Revise los requisitos del sistema y las topologías de red para usar las redes de vSphere para el Supervisor con NSX Advanced Load Balancer. Consulte Requisitos para supervisor zonal con NSX y NSX Advanced Load Balancer, y Requisitos para la implementación de clúster supervisor con NSX y NSX Advanced Load Balancer en *Planificación y conceptos del plano de control de IaaS de vSphere*.

Procedimiento

1 En vSphere Client, desplácese hasta un centro de datos.

2 Haga clic con el botón derecho en el centro de datos y seleccione **Conmutador distribuido > Nuevo conmutador distribuido**.

3 Introduzca un nombre para el conmutador, por ejemplo, **`wcp_vds_1`** y haga clic en **Siguiente**.

4 Seleccione la versión 8.0 para el conmutador y haga clic en **Siguiente**.

5 En **Nombre del grupo de puertos**, introduzca **`Red de cargas de trabajo principal`**, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

   Se creará un conmutador distribuido nuevo con un grupo de puertos en el centro de datos. Este grupo de puertos se podrá utilizar como la red de cargas de trabajo principal de la instancia de Supervisor que creará. La red de cargas de trabajo principal controla el tráfico de las máquinas virtuales del plano de control de Kubernetes.

6 Cree grupos de puertos distribuidos para las redes de cargas de trabajo.

   La cantidad de grupos de puertos que cree dependerá de la topología que desee implementar para Supervisor. Para una topología con una red de cargas de trabajo aislada, cree un grupo de puertos distribuidos que se utilizará como red para todos los espacios de nombres en Supervisor. En el caso de una topología con redes aisladas para cada espacio de nombres, cree la misma cantidad de grupos de puertos que de los espacios de nombres que creará.

   a Vaya al conmutador distribuido que se acaba de crear.

   b Haga clic con el botón derecho en el conmutador y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

c Escriba un nombre para el grupo de puertos, por ejemplo, **`Red de cargas de trabajo`**, y haga clic en **Siguiente**.

d Deje los valores predeterminados, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

7 Cree un grupo de puertos para la red de datos .

a Haga clic con el botón derecho en el conmutador distribuido y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

b Escriba un nombre para el grupo de puertos, por ejemplo, **`Red de datos`**, y haga clic en **Siguiente**.

c En la página **Configurar parámetros**, introduzca las propiedades generales del nuevo grupo de puertos distribuidos y haga clic en **Siguiente**.

Propiedad	Descripción
Enlace de puertos	Elija cuándo se deben asignar los puertos a las máquinas virtuales conectadas a este grupo de puertos distribuidos. Seleccione **Enlace estático** para asignar un puerto a una máquina virtual cuando la máquina virtual se conecta al grupo de puertos distribuidos.
Asignación de puertos	Seleccione la asignación de puertos **Elástico**. El número predeterminado de puertos es ocho. Cuando se asignan todos los puertos, se crea un nuevo conjunto de ocho puertos.
Cantidad de puertos	Conserve el valor predeterminado .
Grupo de recursos de red	En el menú desplegable, asigne el nuevo grupo de puertos distribuidos a un grupo de recursos de red definido por el usuario . Si no creó un grupo de recursos de red, el menú está vacío.
VLAN	En el menú desplegable, seleccione el tipo de filtrado y marcado del tráfico de VLAN: ■ **Ninguna**: no utilice la VLAN. Seleccione esta opción si utiliza el etiquetado de conmutador externo . ■ **VLAN**: en el cuadro de texto ID de VLAN, escriba un valor de 1 a 4094 para el etiquetado de conmutador virtual. ■ **Enlace troncal de VLAN**: utilice esta opción para el etiquetado de invitado virtual y para pasar el tráfico de VLAN con un identificador al SO invitado. Escriba un rango troncal de VLAN. Puede configurar varios rangos o VLAN individuales con una lista separada por comas. Por ejemplo, `1702-1705`, `1848-1849`. ■ **VLAN privada**: asocie el tráfico a una VLAN privada creada en el conmutador distribuido. Si no creó ninguna VLAN privada, este menú estará vacío.
Avanzado	Deje esta opción sin seleccionar.

8 En la página **Listo para finalizar**, revise la configuración y haga clic en **Finalizar**.

Resultados

Se crea el conmutador distribuido y los grupos de puertos distribuidos aparecen en el conmutador distribuido.

Implementar y configurar NSX Manager

Utilice vSphere Client para implementar NSX Manager en el clúster de vSphere. A continuación, puede configurar y utilizar NSX Manager para administrar el entorno de NSX.

Requisitos previos

- - Compruebe que el entorno cumpla con los requisitos de red. Para obtener información sobre los requisitos, consulte Requisitos para supervisor zonal con NSX y NSX Advanced Load Balancer y Requisitos para la implementación de clústeres en supervisor con NSX y NSX Advanced Load Balancer en *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Compruebe que los puertos necesarios estén abiertos. Para obtener información sobre los puertos y los protocolos, consulte la *Guía de instalación de NSX*.

Procedimiento

1. Busque el archivo OVA de NSX en el portal de descargas de VMware.

   Copie la URL de descarga o descargue el archivo OVA.
2. Haga clic con el botón secundario del ratón y seleccione **Implementar plantilla de OVF** para iniciar el Asistente de instalación.
3. En la pestaña **Seleccione una plantilla de archivo OVF**, introduzca la URL de descarga de OVA o desplácese hasta el archivo OVA.
4. En la pestaña **Seleccionar un nombre y una carpeta**, escriba un nombre para la máquina virtual de NSX Manager.
5. En la pestaña **Seleccionar un recurso informático**, seleccione el clúster de vSphere en el que se implementará NSX Manager.
6. Haga clic en **Siguiente** para revisar los detalles.
7. En la pestaña **Configuración**, seleccione el tamaño de implementación de NSX.
8. En la pestaña **Seleccionar almacenamiento**, seleccione el almacenamiento compartido para la implementación.
9. Para habilitar el aprovisionamiento fino, seleccione **Aprovisionamiento fino** en **Seleccionar formato de disco virtual**.

   Los discos virtuales cuentan con aprovisionamiento grueso de forma predeterminada.
10. En la pestaña **Seleccionar redes**, seleccione el grupo de puertos de administración o la red de destino para NSX Manager en **Red de destino**.

    Por ejemplo, `DPortGroup-MGMT`.

11 En la pestaña **Personalizar plantilla**, introduzca la raíz del sistema, el administrador de la CLI y las contraseñas de auditoría de NSX Manager. Las contraseñas deben cumplir con las restricciones de seguridad para contraseñas.

   - Al menos 12 caracteres.
   - Al menos una letra en minúsculas.
   - Al menos una letra en mayúsculas.
   - Al menos un dígito.
   - Al menos un carácter especial.
   - Al menos cinco caracteres diferentes.
   - El módulo PAM de Linux aplica las reglas de complejidad de contraseña predeterminadas.

12 Introduzca la puerta de enlace IPv4 predeterminada, la red de administración IPv4, la máscara de red de la red de administración, el servidor DNS, la lista de búsqueda de dominios y la dirección IP de NTP.

13 Habilite SSH y permita el inicio de sesión SSH raíz en la línea de comandos de NSX Manager.

   De forma predeterminada, las opciones SSH están deshabilitadas por motivos de seguridad.

14 Compruebe que la especificación de la plantilla de OVF personalizada sea correcta y haga clic en **Finalizar** para iniciar la instalación.

15 Después de que arranque NSX Manager, inicie sesión en la CLI como administrador y ejecute el comando `get interface eth0` para comprobar que la dirección IP se aplicó según lo previsto.

16 Introduzca el comando `get services` para comprobar que se están ejecutando todos los servicios.

Implementar nodos de NSX Manager para formar un clúster

Un clúster de NSX Manager proporciona alta disponibilidad. Los nodos de NSX Manager solo se pueden implementar mediante la interfaz de usuario en los hosts ESXi que administra vCenter Server. Para crear un clúster de NSX Manager, implemente dos nodos adicionales con la finalidad de formar un clúster de tres nodos en total. Cuando se implementa un nodo nuevo desde la interfaz de usuario, este se conecta al primer nodo implementado para formar un clúster. Todos los detalles del repositorio y la contraseña del primer nodo implementado se sincronizan con el nodo que se acaba de implementar.

Requisitos previos

- Compruebe que se haya instalado un nodo de NSX Manager.
- Compruebe que se haya configurado un administrador de equipo.
- Compruebe que los puertos necesarios estén abiertos.
- Compruebe que se haya configurado un almacén de datos en el host ESXi.

- Compruebe que tenga la dirección IP y la puerta de enlace, las direcciones IP del servidor DNS, la lista de búsqueda de dominios y la dirección IP del servidor NTP que utilizará NSX Manager.
- Compruebe que tenga una red de grupos de puertos de máquina virtual de destino. Coloque los dispositivos de NSX en una red de máquinas virtuales de administración.

Procedimiento

1 Desde un explorador, inicie sesión con privilegios de administrador en NSX Manager en https://<manager-ip-address>.

2 Para implementar un dispositivo, seleccione **Sistema > Dispositivos > Agregar NSX Appliance**.

3 Introduzca los detalles del dispositivo.

Opción	Descripción
Nombre de host	Introduzca el nombre del host o el FQDN que se utilizará para el nodo.
Dirección IP/máscara de red de administración	Introduzca una dirección IP que se asignará al nodo.
Puerta de enlace de administración	Introduzca una dirección IP de puerta de enlace que vaya a utilizar el nodo.
Servidores DNS	Introduzca la lista de direcciones IP del servidor DNS que vaya a utilizar el nodo.
Servidor NTP	Introduzca la lista de direcciones IP del servidor NTP.
Tamaño del nodo	Seleccione el formato **Mediano (6 vCPU, 24 GB de RAM, 300 GB de almacenamiento)** en las opciones.

4 Introduzca los detalles de configuración del dispositivo.

Opción	Descripción
Administrador de equipo	Seleccione la instancia de vCenter Server que configuró como administrador de equipo.
Clúster de proceso	Seleccione el clúster al que se debe unir el nodo.
Almacén de datos	Seleccione un almacén de datos para los archivos de nodo.
Formato de disco virtual	Seleccione el formato **Aprovisionamiento fino**.
Red	Haga clic en **Seleccionar red** para seleccionar la red de administración del nodo.

5 Introduzca los detalles de acceso y las credenciales.

Opción	Descripción
Habilitar SSH	Active el botón para permitir el inicio de sesión SSH en el nodo nuevo.
Habilitar el acceso raíz	Active el botón para permitir el acceso raíz en el nodo nuevo.

Opción	Descripción
Credenciales raíz del sistema	Establezca la contraseña raíz y confírmela para el nodo nuevo. La contraseña debe cumplir las restricciones de seguridad para contraseñas. ■ Al menos 12 caracteres. ■ Al menos una letra en minúsculas. ■ Al menos una letra en mayúsculas. ■ Al menos un dígito. ■ Al menos un carácter especial. ■ Al menos cinco caracteres diferentes. ■ El módulo PAM de Linux aplica las reglas de complejidad de contraseña predeterminadas.
Credenciales de la CLI de administración y credenciales de la CLI de auditoría	Seleccione la casilla de verificación **Igual que la contraseña raíz** si desea usar la misma contraseña que configuró para la raíz; de lo contrario, anule la selección de esta casilla y establezca otra contraseña diferente.

6 Haga clic en **Instalar dispositivo**.

   Se implementará el nodo nuevo. Puede realizar un seguimiento del proceso de implementación en la página **Sistema> > Dispositivos**. No agregue más nodos hasta que finalice la instalación y el clúster esté estable.

7 Espere a que finalice la implementación, la creación del clúster y la sincronización del repositorio.

   El proceso de unión y estabilización del clúster puede tardar entre 10 y 15 minutos. Compruebe que el estado de cada grupo de servicios del clúster sea `ACTIVO` antes de realizar cualquier otro cambio en el clúster.

8 Después de que arranque el nodo, inicie sesión en la CLI como administrador y ejecute el comando `get interface eth0` para comprobar que la dirección IP se aplicó según lo previsto.

9 Si el clúster solo tiene dos nodos, agregue otro dispositivo. Seleccione **Sistema > Dispositivos > Agregar NSX Appliance** y repita los pasos de configuración.

Agregar una licencia

Agregue una licencia mediante el NSX Manager.

Requisitos previos

Obtenga una licencia Avanzada o superior de NSX.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Licencias > Agregar**.

3 Introduzca la clave de licencia.

4 Haga clic en **Agregar**.

Agregar un administrador de equipo

Un administrador de equipo es una aplicación que gestiona recursos como hosts y máquinas virtuales. Configure la instancia de vCenter Server que está asociada con la instancia de NSX como administrador de equipo en NSX Manager.

Para obtener más información, consulte la *Guía de administración de NSX*.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Administradores de equipo > Agregar**

3 Introduzca los detalles del administrador de equipo.

Opción	Descripción
Nombre y descripción	Introduzca el nombre y la descripción del vCenter Server.
Tipo	El tipo predeterminado es VMware vCenter.
Varias instancias de NSX	Deje esta opción sin seleccionar. La opción de varias instancias de NSX permite registrar la misma instancia de vCenter Server con varias instancias de NSX Manager. Esta opción no es compatible en los clústeres de Supervisor y vSphere Lifecycle Manager.
FQDN o dirección IP	Introduzca el FQDN o la dirección IP de la instancia del vCenter Server.
Puerto HTTPS del proxy inverso	El puerto predeterminado es 443. Si utiliza otro puerto, compruebe que el puerto esté abierto en todos los dispositivos de NSX Manager. Establezca el puerto de proxy inverso para registrar el administrador de equipos en NSX.
Nombre de usuario y contraseña	Introduzca las credenciales de inicio de sesión de vCenter Server.
Huella digital de SHA-256	Escriba el valor del algoritmo de huella digital SHA-256 de vCenter Server.

Puede mantener los valores predeterminados para los demás ajustes.

Si deja el valor de huella digital en blanco, se le solicitará que acepte la huella digital que proporciona el servidor. Tras aceptar la huella digital, NSX tarda unos segundos en detectar y registrar los recursos de vCenter.

4 Seleccione **Habilitar confianza** para permitir que vCenter Server se comunique con NSX.

5 Si no proporcionó un valor de huella digital para NSX Manager, el sistema identificará la huella digital y la mostrará.

6 Haga clic en **Agregar** para aceptar la huella digital.

Resultados

Después de cierto tiempo, el administrador de equipos se registra en vCenter Server y el estado de la conexión cambia a `Activo`. Si el FQDN o el PNID de vCenter Server cambian, debe volver a registrarlos en NSX Manager. Para obtener más información, consulte Registrar vCenter Server en NSX Manager.

Nota Después de que el vCenter Server se registre correctamente, no apague ni elimine la máquina virtual de NSX Manager sin eliminar primero el administrador de equipo. De lo contrario, cuando implemente un nuevo NSX Manager, no podrá volver a registrar el mismo vCenter Server. Recibirá un error que indica que vCenter Server ya se registró en otra instancia de NSX Manager.

Puede hacer clic en el nombre del administrador de equipo para ver los detalles, editar el administrador de equipo o administrar las etiquetas que se aplican al administrador de equipo.

Crear zonas de transporte

Las zonas de transporte indican los hosts y las máquinas virtuales que pueden utilizar una red determinada. Una zona de transporte puede abarcar uno o varios clústeres de host.

Utilice las zonas de transporte predeterminadas o cree las siguientes zonas:

- Una zona de transporte superpuesta que las máquinas virtuales del plano de control de Supervisor utilizan para la conectividad de red de administración entre NSX Advanced Load Balancer Controller y los motores de servicio.
- Una zona de transporte de VLAN para los nodos de NSX Edge que se utilizará para los vínculos superiores a la red física.

Procedimiento

1. Inicie sesión en NSX Manager.
2. Seleccione **Sistema > Tejido > Zonas de transporte > AGREGAR ZONA DE TRANSPORTE**.
3. Introduzca un nombre para la zona de transporte y, opcionalmente, una descripción. Por ejemplo, **`overlayTZ`**.
4. Seleccione el tipo de tráfico **Superpuesto**.

   Las siguientes zonas de transporte existen de forma predeterminada:

   - Una zona de transporte de VLAN con el nombre `nsx-vlan-transportzone`.
   - Una zona de transporte superpuesta con el nombre `nsx-overlay-transportzone`.
5. Haga clic en **GUARDAR**.
6. Repita los pasos del 2 al 5 para crear una zona de transporte con el nombre **`vlanTZ`** y el tipo de tráfico **VLAN**.

7 (opcional) Introduzca uno o varios nombres de directiva de formación de equipos de enlace ascendente.

   Los segmentos asociados a las zonas de transporte usan estas directivas de formación de equipos con nombre. Si los segmentos no encuentran una directiva de formación de equipos con nombre que coincida, se utilizará la directiva de formación de equipos de vínculo superior predeterminada.

Resultados

Las zonas de transporte que creó aparecen en la página **Zonas de transporte**.

Crear un grupo de direcciones IP para las direcciones IP del endpoint de túnel del host

Cree grupos de direcciones IP para los endpoints de túnel (Tunnel Endpoints, TEP) del host ESXi. Los TEP son las direcciones IP de origen y destino que se utilizan en el encabezado IP externo para identificar los hosts ESXi que originan y finalizan la encapsulación NSX de tramas superpuestas.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Redes > Grupos de direcciones IP > AGREGAR GRUPO DE DIRECCIONES IP**.

3 Introduzca un nombre y una descripción opcional para el grupo de direcciones IP. Por ejemplo, `ESXI-TEP-IP-POOL`.

4 Haga clic en **Establecer**.

5 Seleccione **Rangos de IP** en el menú desplegable **AGREGAR SUBRED**.

6 Introduzca los siguientes detalles del grupo de direcciones IP.

Opción	Descripción
Rangos de IP	Introduzca el rango de asignación de IP. Por ejemplo, `IPv4 Range - 192.168.12.1-192.168.12.60, IPv6 Range - 2001:800::0001-2001:0fff:ffff:ffff:ffff:ffff:ffff:ffff`
CIDR	Introduzca la dirección de red en una notación CIDR. Por ejemplo, `192.23.213.0/24`.

7 De manera opcional, introduzca los siguientes detalles.

Opción	Descripción
Descripción	Introduzca la descripción para el rango de IP.
IP de puerta de enlace	Introduzca la dirección IP de la puerta de enlace. Por ejemplo, `192.23.213.253`.

Opción	Descripción
Servidores DNS	Introduzca la dirección del servidor DNS.
Sufijo DNS	Introduzca el sufijo DNS.

8 Haga clic en **AGREGAR** y **APLICAR**.

9 Haga clic en **GUARDAR**.

Resultados

Compruebe que los grupos de direcciones IP de TEP que creó aparezcan en la página Grupo de direcciones IP.

Cree un grupo de direcciones IP para nodos de Edge

Cree grupos de direcciones IP para los nodos de Edge. No es necesario que las direcciones de TEP se puedan enrutar. Puede utilizar cualquier esquema de direcciones IP que permita al TEP de Edge comunicarse con el TEP del host.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Redes > Grupos de direcciones IP > AGREGAR GRUPO DE DIRECCIONES IP**.

3 Introduzca un nombre y una descripción opcional para el grupo de direcciones IP. Por ejemplo, **`EDGE-TEP-IP-POOL`**.

4 Haga clic en **Establecer**.

5 Introduzca los siguientes detalles del grupo de direcciones IP.

Opción	Descripción
Rangos de IP	Introduzca el rango de asignación de IP. Por ejemplo, `IPv4 Range - 192.168.12.1-192.168.12.60`, `IPv6 Range - 2001:800::0001-2001:0fff:ffff:ffff:ffff:ffff:ffff:ffff`
CIDR	Introduzca la dirección de red en una notación CIDR. Por ejemplo, `192.23.213.0/24`.

6 De manera opcional, introduzca los siguientes detalles.

Opción	Descripción
Descripción	Introduzca la descripción para el rango de IP.
IP de puerta de enlace	Introduzca la dirección IP de la puerta de enlace. Por ejemplo, `192.23.213.253`.
Servidores DNS	Introduzca la dirección del servidor DNS.
Sufijo DNS	Introduzca el sufijo DNS.

7 Haga clic en **AGREGAR** y **APLICAR**.

8 Haga clic en **GUARDAR**.

Resultados

Compruebe que los grupos de direcciones IP que creó aparezcan en la página Grupo de direcciones IP.

Crear un perfil de host de vínculo superior de ESXi

Un perfil de host de vínculo superior define las directivas para los vínculos superiores de los hosts de ESXi a los segmentos de NSX.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de vínculo superior > AGREGAR PERFIL**.

3 Introduzca un nombre para el perfil de vínculo superior y, si lo desea, una descripción del perfil de vínculo superior.

   Por ejemplo, **`ESXI-UPLINK-PROFILE`**.

4 En la sección **Formación de equipos**, haga clic en **AGREGAR** para agregar un nombre a la directiva de formación de equipos y configure una directiva **FAILOVER_ORDER**.

   Se especifica una lista de los vínculos superiores activos y cada interfaz en el nodo de transporte está fijada a un vínculo superior activo. Esta configuración permite el uso de varios vínculos superiores activos al mismo tiempo.

5 Configure vínculos activos y en espera.

   Por ejemplo, configure **`uplink-1`** como el vínculo superior activo y **`uplink-2`** como el vínculo superior en espera.

6 (opcional) Introduzca un valor de VLAN de transporte. Por ejemplo, **`1060`**.

   El endpoint de túnel (Tunnel Endpoint, TEP) utiliza la VLAN de transporte establecida en el tráfico de superposición de etiquetas de perfil de vínculo superior y el identificador de VLAN.

7 Introduzca el valor de MTU. El valor debe ser al menos 1600, pero no mayor que el valor de MTU en los conmutadores físicos y vSphere Distributed Switch.

   NSX toma el valor de MTU predeterminado global de 1700.

Resultados

Consulte los vínculos superiores en la página **Perfil de vínculo superior**.

Crear un perfil de vínculo superior de NSX Edge

Un vínculo superior es un vínculo de los nodos de NSX Edge a los conmutadores lógicos de NSX. Un perfil de vínculo superior define directivas para los vínculos superiores al establecer directivas de formación de equipos, vínculos activos y en espera, identificador de VLAN de transporte y valor de MTU.

Cree un perfil de vínculo superior con la directiva de formación de equipos de orden de conmutación por error con un vínculo superior activo para el tráfico de superposición de máquinas virtuales de Edge.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de vínculo superior > AGREGAR PERFIL > ..**

3 Introduzca un nombre para el perfil de vínculo superior y, si lo desea, una descripción del perfil de vínculo superior.

   Por ejemplo, **`EDGE-UPLINK-PROFILE`**.

4 En la sección **Formación de equipos**, haga clic en **AGREGAR** para agregar un nombre a la directiva de formación de equipos y configure una directiva **FAILOVER_ORDER**.

   Se especifica una lista de los vínculos superiores activos y cada interfaz en el nodo de transporte está fijada a un vínculo superior activo. Esta configuración permite el uso de varios vínculos superiores activos al mismo tiempo.

5 Configure un vínculo superior activo.

   Por ejemplo, configure **`uplink-1`** como vínculo superior activo.

Resultados

Consulte los vínculos superiores en la página **Perfil de vínculo superior**.

Crear un perfil de nodo de transporte

Un perfil de nodo de transporte define cómo se instala y configura NSX en los hosts de un clúster en particular al que está conectado el perfil. Cree un perfil de nodo de transporte antes de preparar clústeres de ESXi como nodos de transporte.

Nota Los perfiles de nodo de transporte solo se aplican a hosts. No se pueden aplicar a los nodos de transporte de Edge de NSX.

Requisitos previos

- Compruebe que haya un clúster disponible. Consulte Implementar nodos de NSX Manager para formar un clúster.
- Cree una zona de transporte superpuesta. Consulte Crear zonas de transporte.
- Configure un grupo de direcciones IP. Consulte Crear un grupo de direcciones IP para las direcciones IP del endpoint de túnel del host.
- Agregue un administrador de equipo. Consulte Agregar un administrador de equipo.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Hosts**.

3 En la página **Hosts**, seleccione **Perfil de nodo de transporte > AGREGAR PERFIL DE NODO DE TRANSPORTE**.

4 Introduzca un nombre para introducir el perfil de nodo de transporte. Por ejemplo, **HOST-TRANSPORT-NODE-PROFILE**.

   Opcionalmente, puede agregar la descripción sobre el perfil de nodo de transporte.

5 En el campo **Conmutador de host**, seleccione **Establecer**.

6 En la ventana **Conmutador de host**, introduzca los detalles del conmutador.

Opción	Descripción
vCenter	Seleccione el vCenter Server.
Tipo	Indique el tipo de conmutador que se configurará en el host. Seleccione **VDS**.
VDS	Seleccione el VDS creado en la instancia de vCenter Server seleccionada. Por ejemplo, **wcp_vds_1**.
Zonas de transporte	Seleccione la zona de transporte superpuesta creada anteriormente. Por ejemplo, **overlayTZ**.
Perfil de vínculo superior	Seleccione el perfil de host de vínculo superior creado anteriormente. Por ejemplo, **ESXI-UPLINK-PROFILE**.
Tipo de dirección IP	Seleccione **IPv4**.
Asignación de IPv4	Seleccione **Usar grupo de direcciones IP**.
Grupo de IPv4	Seleccione el grupo de TEP de host creado anteriormente. Por ejemplo, **ESXI-TEP-IP-POOL**.
Asignación de vínculo superior de directiva de formación de equipos	Haga clic en **Agregar** y asigne los vínculos superiores definidos en el perfil de vínculo superior NSX a los vínculos superiores vSphere Distributed Switch. Por ejemplo, asigne **uplink-1** a **Vínculo superior 1** y **uplink-2** a **Vínculo superior 2**.

7 Haga clic en **AGREGAR** y **APLICAR**.

8 Haga clic en **GUARDAR** para guardar la configuración.

Resultados

El perfil que creó está incluido en la página **Perfiles de nodo de transporte**.

Crear un perfil de clúster de NSX Edge

Cree un perfil de clúster de NSX Edge que defina las directivas del nodo de transporte de NSX Edge.

Requisitos previos

Compruebe que el clúster de NSX Edge esté disponible.

Procedimiento

1 Inicie sesión en NSX Manager.
2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de clúster de Edge > AGREGAR PERFIL > .**.
3 Introduzca los detalles del perfil de clúster de NSX Edge.
4 Introduzca un nombre de perfil para el clúster de NSX Edge. Por ejemplo, **`Perfil de clúster: 1`**.

   Opcionalmente, introduzca una descripción.
5 Deje los valores predeterminados para el resto de los ajustes.
6 Haga clic en **AGREGAR**.

Configurar NSX en el clúster

Para instalar NSX y preparar la superposición de TEP, aplique el perfil de nodo de transporte al clúster de vSphere.

Requisitos previos

Compruebe que se creó un perfil de nodo de transporte.

Procedimiento

1 Inicie sesión en NSX Manager.
2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de host**.
3 En el menú desplegable **Administrado por**, seleccione un vCenter Server existente.

   La página muestra los clústeres de vSphere disponibles.
4 Seleccione el clúster de proceso en el que desea configurar NSX.
5 Haga clic en **Configurar NSX**.
6 Seleccione el perfil de nodo de transporte creado previamente y haga clic en **Aplicar**.

   Por ejemplo, `HOST-TRANSPORT-NODE-PROFILE`.
7 En la página **Nodo de transporte de host**, compruebe que el estado de configuración de NSX sea `Success` y que el estado de conectividad de los hosts en el clúster de NSX Manager sea `Up`.

Resultados

El perfil de nodo de transporte creado anteriormente se aplica al clúster de vSphere para instalar NSX y preparar la superposición de los TEP.

Crear un nodo de transporte de NSX Edge

Puede agregar una máquina virtual de NSX Edge al tejido de NSX y proceder a configurarla como una máquina virtual de nodo de transporte de NSX Edge.

Requisitos previos

Compruebe que haya creado las zonas de transporte, el perfil de enlace ascendente de Edge y el grupo de direcciones IP de TEP de Edge.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de Edge > AGREGAR NODO DE EDGE**.

3 En **Nombre y descripción**, introduzca un nombre para el nodo de NSX Edge.

   Por ejemplo, `nsx-edge-1`

4 Introduzca el nombre de host o FQDN de vCenter Server.

   Por ejemplo, `nsx-edge-1.lab.com`.

5 Seleccione el formato para el dispositivo de máquina virtual de NSX Edge.

6 En **Credenciales**, introduzca la CLI y las contraseñas raíz de NSX Edge. Las contraseñas deben cumplir con las restricciones de seguridad para contraseñas.

   - Al menos 12 caracteres.
   - Al menos una letra en minúsculas.
   - Al menos una letra en mayúsculas.
   - Al menos un dígito.
   - Al menos un carácter especial.
   - Al menos cinco caracteres diferentes.
   - El módulo PAM de Linux aplica las reglas de complejidad de contraseña predeterminadas.

7 Habilite **Permitir inicio de sesión SSH** para las credenciales raíz y de CLI.

8 En **Configurar implementación**, configure las siguientes propiedades:

Opción	Descripción
Administrador de equipo	Seleccione el administrador de equipo en el menú desplegable. Por ejemplo, seleccione `vCenter`.
Clúster	Seleccione el clúster en el menú desplegable. Por ejemplo, seleccione `Compute-Cluster`.
Almacén de datos	Seleccione el almacén de datos compartido de la lista. Por ejemplo, `vsanDatastore`.

9 Configure los ajustes del nodo.

Opción	Descripción
Asignación de IP	Seleccione Estática. Introduzca los valores de: ■ **IP de administración**: introduzca la dirección IP en la misma VLAN que la red de administración de vCenter Server. Por ejemplo, `10.197.79.146/24`. ■ **Puerta de enlace predeterminada**: la puerta de enlace predeterminada de la red de administración. Por ejemplo, `10.197.79.253`.
Interfaz de administración	Haga clic en **Seleccionar interfaz** y, a continuación, seleccione el grupo de puertos de vSphere Distributed Switch en la misma VLAN de la red de administración en el menú desplegable que creó anteriormente. Por ejemplo, `DPortGroup-MGMT`.

10 En **Configurar NSX**, haga clic en **Agregar conmutador** para configurar las propiedades del conmutador.

11 Utilice el nombre predeterminado para el **Nombre del conmutador de Edge**.

Por ejemplo, `nvds1`.

12 Seleccione la zona de transporte a la que pertenece el nodo de transporte.

Seleccione las zonas de transporte superpuestas creadas anteriormente.

Por ejemplo, `overlayTZ`.

13 Seleccione el perfil de vínculo superior de Edge creado anteriormente.

Por ejemplo, `EDGE-UPLINK-PROFILE`.

14 Seleccione **Usar grupo de IP** en **Asignación de IP**.

15 Seleccione el grupo de IP de TEP de Edge creado anteriormente.

Por ejemplo, `EDGE-TEP-IP-POOL`.

16 En la sección **Asignación de conmutador de directiva de formación de equipos**, asigne el vínculo superior a los perfiles de vínculo superior de Edge creados anteriormente.

Por ejemplo, para `Uplink1`, seleccione `uplink-1`.

17 Repita los pasos 10 a 16 para agregar un conmutador nuevo.

Por ejemplo, configure los siguientes valores:

Propiedad	Valor
Nombre del conmutador de Edge	`nvds2`
Zona de transporte	`vlanTZ`

Propiedad	Valor
Perfil de vínculo superior de Edge	`EDGE-UPLINK-PROFILE`
Asignación de conmutador de directiva de formación de equipos	`DPortGroup-EDGE-UPLINK`

18 Haga clic en **Finalizar**.

19 Repita los pasos 2 a 18 para una segunda máquina virtual de NSX Edge.

20 Consulte el estado de conexión en la página **Nodos de transporte de Edge**.

Crear un clúster de NSX Edge

Para asegurarse de que al menos un NSX Edge siempre esté disponible, cree un clúster de NSX Edge.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema** > **Tejido** > **Nodos** > **Clústeres de Edge** > **Agregar**.

3 Introduzca el nombre del clúster NSX Edge.

   Por ejemplo, `EDGECLUSTER1`.

4 Haga clic en **GUARDAR**.

5 Seleccione el perfil de clúster de NSX Edge que configuró en el menú desplegable. Por ejemplo, **`Perfil de clúster: 1`**.

6 En el menú desplegable **Tipo de miembro**, seleccione el **nodo de Edge**.

7 En la columna **Disponible**, seleccione las máquinas virtuales de NSX Edge creadas previamente y haga clic en la flecha derecha para moverlas a la columna **Seleccionada**.

8 Por ejemplo, `nsx-edge-1` y `nsx-edge-2`.

9 Haga clic en **Guardar**.

Pasos siguientes

Crear una puerta de enlace de nivel 0

La puerta de enlace de nivel 0 es el enrutador lógico de NSX que proporciona conectividad de norte a sur para las redes lógicas de NSX a la infraestructura física. vSphere IaaS control plane admite varias puertas de enlace de nivel 0 en distintos clústeres de NSX Edge en la misma zona de transporte.

Para obtener más información sobre cómo configurar mapas de rutas de NSX en el enrutador de nivel 0 de Edge, consulte la *Guía de operaciones y administración de VMware Cloud Foundation* en https://docs.vmware.com/es/VMware-Cloud-Foundation/4.0/vcf-40-doc.zip.

Requisitos previos

Compruebe que se creó un clúster de NSX Edge.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Redes > Puertas de enlace de nivel 0**.

3 Haga clic en **AGREGAR PUERTA DE ENLACE**.

4 Introduzca un nombre para la puerta de enlace de nivel 0.

   Por ejemplo, `ContainerT0`.

5 Seleccione un modo HA activo-en espera.

   El modo predeterminado es activo-activo. En el modo activo-en espera, el miembro activo elegido procesa todo el tráfico. Si se produce un error en el miembro activo, se elige un nuevo miembro para que esté activo.

6 Si el modo de alta disponibilidad es activo-en espera, seleccione un modo de conmutación por error.

Opción	Descripción
Preferente	Si se produce un error en el nodo preferente y se soluciona, reemplazará al nodo del mismo nivel y se convertirá en el nodo activo. El estado de este nodo cambiará a en espera.
No preferente	Si se produce un error en el nodo preferente y se soluciona, comprobará si el nodo del mismo nivel es el activo. Si es así, el nodo preferente no reemplazará al nodo del mismo nivel y será el nodo que esté en espera.

7 Seleccione el clúster de NSX Edge creado anteriormente.

   Por ejemplo, seleccione `Cluster Profile - 1`.

8 Haga clic en **Guardar**.

   Se crea la puerta de enlace de nivel 0.

9 Seleccione **Sí** para continuar con la configuración.

10 Configure interfaces.

   a Expanda **Interfaces** y haga clic en **Establezca la opción**.

   b Haga clic en **Agregar interfaz**.

   c Escriba un nombre.

      Por ejemplo, introduzca el nombre `TIER-0_VWT-UPLINK1`.

   d En **Tipo**, seleccione **Externo**.

e Introduzca una dirección IP del enrutador lógico de Edge – VLAN de vínculo superior. La dirección IP debe ser diferente de la dirección IP de administración configurada para las máquinas virtuales de NSX Edge creadas previamente.

   Por ejemplo, `10.197.154.1/24`.

f En **Conectado a**, seleccione el segmento de vínculo superior de nivel 0 que creó anteriormente.

   Por ejemplo, `TIER-0-LS-UPLINK`

g Seleccione un nodo de NSX Edge de la lista.

   Por ejemplo, `nsx-edge-1`.

h Haga clic en **Guardar**.

i Repita los pasos de "a" a "h" para la segunda interfaz.

   Por ejemplo, cree un segundo `TIER-0_VWT-UPLINK2` de vínculo superior con la dirección IP `10.197.154.2/24` conectado al nodo de `nsx-edge-2` Edge.

j Haga clic en **Cerrar.**

11 Para configurar la alta disponibilidad, haga clic en **Establezca la opción** en **Configuración de VIP de alta disponibilidad**.

a Haga clic en **AGREGAR CONFIGURACIÓN DE VIP DE ALTA DISPONIBILIDAD**.

b Introduzca la dirección IP.

   Por ejemplo, `10.197.154.3/24`

c Seleccione las interfaces.

   Por ejemplo, `TIER-0_WVT-UPLINK1` y `TIER-0_WVT-UPLINK2`.

d Haga clic en **Agregar** y **Aplicar**.

12 Para configurar el enrutamiento, haga clic en **Enrutamiento**.

a Haga clic en **Establecer** en Rutas estáticas.

b Haga clic en **AGREGAR RUTA ESTÁTICA**.

c Escriba un nombre.

   Por ejemplo, `DEFAULT-STATIC-ROUTE`.

d Introduzca `0.0.0.0/0` para la dirección IP de red.

e Para configurar los siguientes saltos, haga clic en **Establecer salto siguiente** y, a continuación, en **Agregar salto siguiente**.

f Introduzca la dirección IP del enrutador del siguiente salto. Suele ser la puerta de enlace predeterminada de la VLAN de la red de administración desde la VLAN de vínculo superior del enrutador lógico de NSX Edge.

   Por ejemplo, `10.197.154.253`.

   g Haga clic en **Agregar**, **Aplicar** y **GUARDAR**.
   h Haga clic en **Cerrar**.

13 (opcional) Seleccione BGP para configurar los detalles locales y del mismo nivel de BGP.
14 Para verificar la conectividad, asegúrese de que un dispositivo externo de la arquitectura física pueda hacer ping en los vínculos superiores que configuró.

Configurar mapas de rutas de NSX en la puerta de enlace de nivel 0 de Edge

Cuando se implementa vSphere IaaS control plane, los mapas de rutas creados en la puerta de enlace de nivel 0 de Edge en modo eBGP contienen un prefijo de IP con solo una regla de denegación. Esto impide que las rutas se anuncien en los conmutadores ToR.

Si utiliza el clúster de Edge solo para Kubernetes: administración de cargas de trabajo, siga la opción 1 y desactive los anuncios de rutas de nivel 1. Si utiliza el clúster de Edge para tareas adicionales, siga la opción 2 y cree una nueva regla de permiso.

Opción 1: Desactivar anuncios de redes conectadas de nivel 1 a través de la puerta de enlace de nivel 0

Las redes conectadas a la puerta de enlace de nivel 1 no se anuncian desde la puerta de enlace de nivel 0 a redes externas.

1 Inicie sesión en el NSX Manager.
2 Seleccione **Redes > Puertas de enlace de nivel 0**.
3 Haga clic en **Editar**.
4 En la sección Subredes de nivel 1 anunciadas, anule la selección de **Interfaces y segmentos conectados**.
5 Haga clic en **Aplicar** y, a continuación, en **Guardar**.

Opción 2: Crear una regla de permiso y aplicarla a la redistribución de rutas

Al implementar vSphere IaaS control plane, se anexa una regla de denegación nueva al mapa de rutas. Por lo tanto, debe agregar una regla de permiso nueva al mapa de rutas para permitir cualquier lista de prefijos IP y mapa de rutas, y aplicarla a la regla de redistribución de rutas como la última regla.

1 Inicie sesión en el NSX Manager.
2 Seleccione **Redes > Puertas de enlace de nivel 0**.
3 Cree una nueva lista de prefijos IP.
   a Expanda **Enrutamiento**.
   b Haga clic en 1 junto a Listas de prefijos de IP.
   c En el cuadro de diálogo Establecer lista de prefijos de IP, haga clic en **Agrezar lista de prefijos de IP**.

d Introduzca un nombre, por ejemplo `test`, y haga clic en **Establecer**.

e Haga clic en **Agregar prefijo**.

f En Red, haga clic en **Cualquiera** y, en Acción, seleccione **Permitir**.

g Haga clic en **Aplicar** y, a continuación, en **Guardar**.

4 Cree un mapa de rutas para la lista de prefijos IP creada en el paso 3.

a Haga clic en **Establecer** junto a Mapa de rutas.

b Haga clic en **Agregar mapa de rutas**.

c Agregue nuevos criterios de coincidencia con el prefijo IP.

d Seleccione el prefijo de IP creado en el paso 3 y la acción **Permitir**.

e Haga clic en **Aplicar** y, a continuación, en **Guardar**.

5 Aplique el mapa de rutas editado a la redistribución de rutas.

a En la página **Puertas de enlace de nivel 0**, expanda **Redistribución de rutas** y haga clic en Editar.

b En el menú desplegable de la columna Mapa de rutas, seleccione el mapa de rutas que creó en el paso 4.

c Haga clic en **Aplicar** y, a continuación, en **Guardar**.

Crear una puerta de enlace de nivel 1

Por lo general, una puerta de enlace de nivel 1 está conectada a una puerta de enlace de nivel 0 en la dirección norte y a los segmentos en la dirección sur.

Requisitos previos

Compruebe que haya creado una puerta de enlace de nivel 0.

Procedimiento

1. Inicie sesión en NSX Manager.
2. Seleccione **Redes > Puertas de enlace de nivel 1**.
3. Haga clic en **AGREGAR PUERTA DE ENLACE DE NIVEL 1**.
4. Introduzca un nombre para la puerta de enlace. Por ejemplo, **`ContainerAviT1`**.
5. Seleccione una puerta de enlace de nivel 0 para conectarse a esta puerta de enlace de nivel 1. Por ejemplo, **`ContainerT0`**.
6. Seleccione el clúster de NSX Edge. Por ejemplo, seleccione **`EDGECLUSTER1`**.
7. Después de seleccionar un clúster de NSX Edge, una opción permite seleccionar nodos de NSX Edge.

8 Seleccione un modo de conmutación por error o acepte la opción predeterminada de **No preferente**.

9 Acepte las opciones predeterminadas para los demás ajustes.

10 Haga clic en **GUARDAR**.

11 (opcional) Configure las interfaces de servicio, las rutas estáticas y los ajustes de multidifusión. Puede aceptar los valores predeterminados.

Crear un segmento de vínculo superior de nivel 0 y un segmento de superposición

El segmento de vínculo superior de nivel 0 proporciona conectividad de norte a sur desde NSX hasta la infraestructura física. El segmento de superposición proporciona la NIC de administración del motor de servicio con la dirección IP.

Requisitos previos

Compruebe que haya creado una puerta de enlace de nivel 0.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Redes > Segmentos > AGREGAR SEGMENTO**.

3 Introduzca un nombre para el segmento.

   Por ejemplo, `TIER-0-LS-UPLINK`.

4 Seleccione la zona de transporte creada previamente.

   Por ejemplo, seleccione `vlanTZ`.

5 Conmute **Estado de administrador** para habilitarlo.

6 Introduzca un identificador de VLAN de la puerta de enlace de nivel 0.

   Por ejemplo, `1089`.

7 Haga clic en **Guardar**.

8 Repita los pasos del 2 al 7 para crear un segmento de superposición `nsxoverlaysegment` con zona de transporte `nsx-overlay-transportzone`.

Instalar y configurar NSX Advanced Load Balancer para vSphere IaaS control plane con NSX

Si utiliza la versión 4.1.1 o posteriores de NSX en el entorno de vSphere IaaS control plane, puede instalar y configurar la versión 22.1.4 o posteriores de NSX Advanced Load Balancer.

- Compruebe que el entorno cumpla con los requisitos para configurar vSphere IaaS control plane con NSX Advanced Load Balancer. Consulte Requisitos para supervisor zonal con NSX y NSX Advanced Load Balancer, y Requisitos para la implementación de clúster supervisor con NSX y NSX Advanced Load Balancer en *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Instale y configure NSX.
- Descargue el OVA de NSX Advanced Load Balancer. VMware proporciona un archivo OVA de NSX Advanced Load Balancer para que lo implemente en el entorno de vSphere en el que habilitará la administración de cargas de trabajo. Descargue la versión más reciente del archivo OVA compatible con vSphere IaaS control plane desde el portal de VMware Customer Connect.

Nota Los procedimientos descritos en esta guía son relevantes para NSX Advanced Load Balancer, que es compatible con vSphere IaaS control plane 8.0 Update 2. Puede haber disponibles versiones posteriores de NSX Advanced Load Balancer, y los flujos de trabajo de la interfaz de usuario podrían ser diferentes.

Para obtener más información sobre NSX Advanced Load Balancer, consulte la Documentación de VMware NSX Advanced Load Balancer.

Importar el archivo OVA de NSX Advanced Load Balancer en una biblioteca de contenido local

Para almacenar la imagen OVA de NSX Advanced Load Balancer, cree una biblioteca de contenido local e importe la imagen en ella.

La creación de una biblioteca de contenido local implica configurar la biblioteca, descargar los archivos OVA e importarlos a la biblioteca de contenido local. Para obtener más información, consulte Usar bibliotecas de contenido.

Requisitos previos

Compruebe que descargó el archivo OVA de NSX Advanced Load Balancer.

Cree una biblioteca de contenido local. Consulte Crear y editar una biblioteca de contenido.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione **Menú > Bibliotecas de contenido**.

3 En la lista de **Bibliotecas de contenido**, haga clic en el vínculo del nombre de la biblioteca de contenido local que haya creado. Por ejemplo, **NSX ALB**.

4 Haga clic en **Acciones**.

5 Seleccione **Importar elemento**.

6 En la ventana **Importar elemento de biblioteca**, seleccione **Archivo local**.

7 Haga clic en **Cargar archivos**.

8 Seleccione el archivo OVA que descargó.

9 Haga clic en **Importar**.

10 Despliegue el panel **Tareas recientes** en la parte inferior de la página.

11 Supervise la tarea **Obtener contenido de un elemento de biblioteca** y compruebe que se haya **Completado** correctamente.

Pasos siguientes

Implemente el controlador de NSX Advanced Load Balancer. Consulte Implementar el controlador de NSX Advanced Load Balancer.

Implementación de NSX Advanced Load Balancer Controller

Implemente la máquina virtual de NSX Advanced Load Balancer Controller en la red de administración de su entorno de vSphere IaaS control plane.

Requisitos previos

- Compruebe que tiene una red de administración en la que implementar NSX Advanced Load Balancer. Puede ser una instancia de vSphere Distributed Switch (vDS) o un conmutador estándar de vSphere (vSS).
- Compruebe que creó un conmutador vDS y un grupo de puertos para la red de datos. Consulte Crear una instancia de vSphere Distributed Switch para un Supervisor para su uso con NSX Advanced Load Balancer.
- Asegúrese de haber completado los requisitos previos. Consulte Requisitos para supervisor zonal con NSX y NSX Advanced Load Balancer, y Requisitos para la implementación de clúster supervisor con NSX y NSX Advanced Load Balancer en *Planificación y conceptos del plano de control de IaaS de vSphere*.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione el clúster de vSphere designado para los componentes de administración.

3 Cree un grupo de recursos denominado **`AVI-LB`**.

4 Haga clic con el botón derecho en el grupo de recursos y seleccione **Implementar plantilla de OVF**.

5 Seleccione **Archivo local** y haga clic en **Cargar archivos**.

6 Busque y seleccione el archivo `controller-VERSION.ova` que descargó como requisito previo.

7 Introduzca un nombre y seleccione una carpeta para la controladora.

Opción	Descripción
Nombre de la máquina virtual	`avi-controller-1`
Ubicación de la máquina virtual	Centro de datos

8 Seleccione el grupo de recursos **`AVI-LB`** como recurso informático.

9 Revise los detalles de la configuración y haga clic en **Siguiente**.

10 Seleccione una **Directiva de almacenamiento de máquina virtual**, como **`vsanDatastore`**.

11 Seleccione la red de administración, por ejemplo, **`red-1`**.

12 Personalice la configuración de la siguiente manera y haga clic **Siguiente** cuando haya terminado.

Opción	Descripción
Dirección IP de la interfaz de administración	Introduzca la dirección IP de la máquina virtual del controlador, como `10.199.17.51`.
Máscara de subred de la interfaz de administración	Introduzca la máscara de subred, como `255.255.255.0`.
Puerta de enlace predeterminada	Introduzca la puerta de enlace predeterminada para la red de administración, como `10.199.17.235`.
Clave de autenticación de inicio de sesión de Sysadmim	Opcionalmente pegue el contenido de una clave pública. Puede dejar la clave en blanco.
Nombre de host del Controlador AVI.	Introduzca el FQDN o la dirección IP del controlador.

13 Revise la configuración de implementación.

14 Haga clic en **Finalizar** para completar la configuración.

15 Utilice vSphere Client para supervisar el aprovisionamiento de la máquina virtual del controlador en el panel **Tareas**.

16 Utilice vSphere Client para encender la máquina virtual del controlador después de implementarla.

Implementar un clúster de controladores

De forma opcional, puede implementar un clúster de tres nodos de controlador. Se recomienda configurar un clúster en entornos de producción para HA y recuperación ante desastres. Si va a ejecutar un controlador de NSX Advanced Load Balancer de un solo nodo, deberá utilizar la función Copia de seguridad y restauración.

Para ejecutar un clúster de tres nodos, después de implementar la primera máquina virtual del controlador, implemente y encienda dos máquinas virtuales del controlador adicionales. No debe ejecutar el asistente de configuración inicial ni cambiar la contraseña de administrador de estos controladores . La configuración de la primera máquina virtual del controlador se asigna a las dos nuevas máquinas virtuales del controlador.

Procedimiento

1 Vaya a **Administración > Controlador**.

2 Seleccione **Nodos**.

3 Haga clic en el icono de edición.

4 Agregue una IP estática para **IP del clúster del controlador**.

Esta dirección IP debe ser de la red de administración .

5 En **Nodos del clúster**, configure los dos nuevos nodos de clúster.

Opción	Descripción
IP	Dirección IP del nodo del controlador .
Nombre	Nombre del nodo. El nombre puede ser la dirección IP .
Contraseña	Contraseña del nodo de controlador . Deje la contraseña vacía.
Dirección IP pública	La dirección IP pública del nodo del controlador . Deje esto vacío.

6 Haga clic en **Guardar**.

Nota Una vez que implemente un clúster, deberá usar la IP del clúster del controlador para cualquier configuración adicional y no la IP del nodo del controlador.

Encender el controlador

Después de implementar la máquina virtual del controlador, podrá encenderla. Durante el proceso de arranque, la dirección IP especificada durante la implementación se asigna a la máquina virtual.

Después de encenderlo, el primer proceso de arranque de la máquina virtual del controlador puede tardar hasta 10 minutos.

Requisitos previos

Implemente el controlador.

Procedimiento

1 En vCenter Server, haga clic con el botón derecho en la máquina virtual `avi-controller-1` que implementó.

2 Seleccione **Encender > Encender**.

A la máquina virtual se le asigna la dirección IP que especificó durante la implementación.

3 Para comprobar si la máquina virtual está encendida, acceda a la dirección IP en un navegador.

   Cuando la máquina virtual se conecta, aparecen advertencias sobre el certificado TLS y la conexión.

4 En la advertencia **Esta conexión no es privada**, haga clic en **Mostrar detalles**.

5 Haga clic en **Visitar este sitio web** en la ventana que aparece.

   Se le solicitarán las credenciales de usuario.

Configurar NSX Advanced Load Balancer Controller

Configure la máquina virtual de NSX Advanced Load Balancer Controller para el entorno de vSphere IaaS control plane.

Para conectar el plano de control del equilibrador de carga con el entorno de vCenter Server, NSX Advanced Load Balancer Controller requiere varios parámetros de configuración posteriores a la implementación.

Requisitos previos

- Compruebe que el entorno cumpla con los requisitos del sistema para configurar NSX Advanced Load Balancer. Consulte Requisitos para supervisor zonal con NSX y NSX Advanced Load Balancer, y Requisitos para la implementación de clúster supervisor con NSX y NSX Advanced Load Balancer en *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Compruebe que dispone de la licencia de nivel Enterprise. El controlador arranca en modo de evaluación, que dispone de todas las funciones equivalentes a las de una licencia de edición Enterprise. Debe asignar una licencia válida de nivel Enterprise al controlador antes de que caduque su período de evaluación.

Procedimiento

1 Con un explorador, diríjase a la dirección IP que especificó al implementar NSX Advanced Load Balancer Controller.

2 Cree una **Cuenta de administrador**.

Opción	Descripción
Nombre de usuario	El nombre de usuario del administrador para la configuración inicial. No puede editar este campo.
Contraseña	Introduzca una contraseña de administrador para la máquina virtual del controlador. La contraseña debe tener al menos 8 caracteres y contener una combinación de caracteres numéricos, caracteres especiales, mayúsculas y minúsculas.

Opción	Descripción
Confirmar contraseña	Vuelva a introducir la contraseña del administrador.
Dirección de correo electrónico (opcional)	Introduzca una dirección de correo electrónico del administrador. Se recomienda proporcionar una dirección de correo electrónico para recuperar la contraseña en un entorno de producción.

3 Ajuste **Configuración del sistema**.

Opción	Descripción
Frase de contraseña	Introduzca una frase de contraseña para la copia de seguridad del controlador. Se realiza una copia de seguridad automática de la configuración del controlador en el disco local de forma periódica. Para obtener más información, consulte Copia de seguridad y restauración. La frase de contraseña debe tener al menos 8 caracteres y contener una combinación de caracteres numéricos, caracteres especiales, mayúsculas y minúsculas.
Confirmar frase de contraseña	Vuelva a introducir la frase de contraseña de copia de seguridad.
Resolutor de DNS	Introduzca una dirección IP para el servidor DNS que está utilizando en el entorno de vSphere IaaS control plane. Por ejemplo, `10.14.7.12`.
Dominios de búsqueda de DNS	Introduzca una cadena de dominio.

4 Asigne una licencia.

a Seleccione **Administración > Licencias**.

b Seleccione **Configuración**.

c Seleccione **Nivel Enterprise** y haga clic en **GUARDAR**.

d Para agregar la licencia, seleccione **Cargar desde equipo**.

Después de cargar el archivo de licencia, aparece en la lista de licencias del controlador. El sistema muestra la información sobre la licencia, incluidas la fecha de inicio y la fecha de caducidad.

5 Para permitir que NSX Advanced Load Balancer Controller se comunique con NSX Manager, cree credenciales de NSX Manager. En el panel de control de NSX Advanced Load Balancer Controller, seleccione **Administración > Credenciales de usuario**.

Opción	Descripción
Nombre	Nombre de las credenciales. Por ejemplo, **`nsxuser`**.
Tipo de credenciales	Seleccione **NSX-T**.
Nombre de usuario	Introduzca el nombre de usuario para iniciar sesión en NSX Manager.
Contraseña	Introduzca la contraseña de NSX Manager.

6 Para permitir que NSX Advanced Load Balancer Controller se comunique con vCenter Server, cree credenciales de vCenter Server.

Opción	Descripción
Nombre	Nombre de las credenciales. Por ejemplo, `vcuser`.
Tipo de credenciales	Seleccione **vCenter**.
Nombre de usuario	Introduzca el nombre de usuario para iniciar sesión en vCenter Server.
Contraseña	Introduzca la contraseña de vCenter Server.

7 Cree un perfil de marcador de posición de IPAM.

Se requiere IPAM para asignar direcciones IP virtuales cuando se crean servicios virtuales.

a En el panel de control de NSX Advanced Load Balancer Controller, seleccione **Plantillas > Perfiles de IPAM/DNS**.

Se mostrará la página **NUEVO PERFIL IPAM/DNS**.

b Introduzca un nombre para el perfil. Por ejemplo, `default-ipam`.

c Seleccione **Tipo** como `Avi Vantage IPAM`.

d Haga clic en **Guardar**.

8 Configure **NSX Cloud**.

a En el panel de control de NSX Advanced Load Balancer Controller, seleccione **Infraestructura > Nubes**.

b Introduzca un nombre para la nube. Por ejemplo, `nsx-cloud`.

c Seleccione **Nube NSX-T** como el tipo de nube.

d Seleccione **DHCP**.

e Introduzca un **Prefijo de nombre de objeto** para los motores de servicio. La cadena de prefijo solo debe tener letras, números y guiones bajos. Este campo no se puede cambiar una vez configurada la nube. Por ejemplo, `nsx`.

9 Introduzca las credenciales de NSX.

a Introduzca la dirección IP de NSX Manager.

b Introduzca las credenciales de NSX Manager que creó. Por ejemplo, `nsxuser`.

10 Configure la red de administración. La red de administración es el canal de comunicación entre NSX Advanced Load Balancer Controller y los motores de servicio.

Opción	Descripción
Zona de transporte	La zona de transporte en la que se ubica el motor de servicio. Seleccione una zona de transporte superpuesta. Por ejemplo, **`nsx-overlay-transportzone`**.
Enrutador lógico de nivel 1	Seleccione la puerta de enlace de nivel 1. Por ejemplo, **`Tier-1_VWT`**.
Segmento de superposición	El segmento de superposición de administración del cual la NIC de administración del motor de servicio obtiene la dirección IP. Por ejemplo, **`nsxoverlaysegment`**.

11 Configure la red de datos.

En la sección **Red de datos**, haga clic en **AGREGAR**.

Opción	Descripción
Zona de transporte	Seleccione una zona de transporte superpuesta. Por ejemplo, **`nsx-overlay-transportzone`**.
Enrutador lógico	Introduzca la puerta de enlace de nivel 1. Por ejemplo, **`Tier-1_VWT`**.
Segmento de superposición	Seleccione el segmento de superposición. Por ejemplo, **`nsxoverlaysegment`**.

12 Introduzca las credenciales para vCenter Server.

En la sección **vCenter Server**, haga clic en **AGREGAR**.

Opción	Descripción
Nombre	Nombre de las credenciales que creó anteriormente. Por ejemplo, **`vcuser`**.
URL	Dirección IP del vCenter Server.

13 Agregue el perfil de IPAM que creó anteriormente. En **Perfil de IPAM**, seleccione **`default-ipam`**.

Se requiere IPAM para asignar direcciones IP virtuales cuando se crean servicios virtuales.

Resultados

Una vez que complete la configuración, verá el **Panel de control** de NSX Advanced Load Balancer Controller. Seleccione **Infraestructura > Nubes** y compruebe que el estado de NSX Advanced Load Balancer Controller para **NSX Cloud** sea de color verde. A veces, el estado puede estar de color amarillo durante un tiempo antes de que cambie a verde hasta que NSX Advanced Load Balancer Controller detecte todos los grupos de puertos en el entorno de vCenter Server.

Pasos siguientes

Configure un grupo de motores de servicio. Consulte Configurar un grupo de motores de servicio.

Configurar un grupo de motores de servicio

vSphere IaaS control plane utiliza **Default-Group** como plantilla para configurar un grupo de motores de servicio por Supervisor. Opcionalmente, puede configurar los motores de servicio **Grupo predeterminado** dentro de un grupo que defina la colocación y el número de máquinas virtuales de motores de servicio en vCenter. También puede configurar la alta disponibilidad si NSX Advanced Load Balancer Controller está en modo Enterprise.

Procedimiento

1 En el panel de la NSX Advanced Load Balancer Controller, seleccione **Infraestructura > Recursos de nube > Grupo de motores de servicio**.

2 En la página **Grupo de motores de servicio**, haga clic en el icono Editar en **Grupo predeterminado**.

   Aparecerá la pestaña **Ajustes generales**.

3 En la sección **Ajustes de alta disponibilidad y colocación**, configure la alta disponibilidad y los servicios virtuales.

   a Seleccione el **Modo de alta disponibilidad**.

      La opción predeterminada es `N + M (buffer)`. Puede mantener el valor predeterminado o seleccionar una de las siguientes opciones:

      - `Active/Standy`
      - `Active/Active`

   b Configure la opción **Número de motores de servicio**. Este es el número máximo de motores de servicio que se pueden crear dentro de un grupo de motores de servicio. El valor predeterminado es **10**.

   c Configure la opción **Colocación de servicios virtuales en los motores de servicio**.

      La opción predeterminada es **Compacto**. Puede seleccionar una de las siguientes opciones:

      - **Distribuido**. NSX Advanced Load Balancer Controller maximiza el rendimiento mediante la colocación de servicios virtuales en los motores de servicio recién encendidos hasta la cantidad máxima de motores de servicio especificados.
      - **Compacto**. NSX Advanced Load Balancer Controller gira los motores de servicios mínimos posibles y coloca el nuevo servicio virtual en un motor de servicio existente. Solo se crea un nuevo motor de servicio cuando se utilizan todos los motores de servicio.

4 Puede mantener los valores predeterminados para los demás ajustes.

5 Haga clic en **Guardar**.

Resultados

El AKO crea un grupo de motores de servicio para cada clúster de vSphere IaaS control plane. La configuración del grupo de motores de servicio se deriva de la configuración del **Grupo predeterminado**. Una vez que el **Grupo predeterminado** esté configurado con los valores necesarios, cualquier nuevo grupo de motores de servicio creado por el AKO tendrá los mismos ajustes. Sin embargo, los cambios realizados en la configuración del **Grupo predeterminado** no se reflejarán en un grupo de motores de servicio ya creado. Debe modificar la configuración de un grupo de motores de servicio existente por separado.

Registrar la NSX Advanced Load Balancer Controller con NSX Manager

Registre la NSX Advanced Load Balancer Controller con NSX Manager.

Requisitos previos

Compruebe que haya implementado y configurado la NSX Advanced Load Balancer Controller.

Procedimiento

1 Inicie sesión en NSX Manager como usuario raíz.

2 Ejecute los siguientes comandos:

```
curl -k --location --request PUT 'https://<nsx-mgr-ip>/policy/api/v1/infra/alb-onboarding-
workflow' \
--header 'X-Allow-Overwrite: True' \
--header 'Authorization: Basic <base64 encoding of username:password of NSX Mgr>' \
--header 'Content-Type: application/json' \
--data-raw '{
"owned_by": "LCM",
"cluster_ip": "<nsx-alb-controller-cluster-ip>",
"infra_admin_username" : "username",
"infra_admin_password" : "password"
}'
```

Si proporciona la configuración de DNS y NTP en la llamada de API, se anula la configuración global. Por ejemplo, `"dns_servers": ["<dns-servers-ips>"]` y `"ntp_servers": ["<ntp-servers-ips>"]`.

Asignar un certificado a NSX Advanced Load Balancer Controller

La NSX Advanced Load Balancer Controller utiliza certificados que envía a los clientes para autenticar sitios y establecer una comunicación segura. Los certificados pueden estar autofirmados por NSX Advanced Load Balancer o crearse como una solicitud de firma del certificado (Certificate Signing Request, CSR) que se envía a una entidad de certificación (Certificate Authority, CA) de confianza, la que genera un certificado de confianza posteriormente. Puede crear un certificado autofirmado o cargar uno externo.

Debe proporcionar un certificado personalizado para habilitar Supervisor. No puede utilizar el certificado predeterminado. Para obtener más información sobre los certificados, consulte Certificados SSL/TLS.

Si utiliza un certificado privado firmado por una entidad de certificación (CA), es posible que la implementación del Supervisor no se complete y que no se aplique la configuración de NSX Advanced Load Balancer. Para obtener más información, consulte La configuración de NSX Advanced Load Balancer no se aplica.

Requisitos previos

Compruebe que la función NSX Advanced Load Balancer esté registrada en NSX Manager.

Procedimiento

1. En el panel de control Controlador, haga clic en el menú de la esquina superior izquierda y seleccione **Plantillas > Seguridad**.
2. Seleccione **Certificados SSL/TLS**.
3. Para crear un certificado, haga clic en **Crear** y seleccione **Certificado de controlador**.

   Aparecerá la ventana **Nuevo certificado (SSL/TLS)**.
4. Introduzca un nombre para el certificado.
5. Si no tiene un certificado válido creado previamente, seleccione **Tipo** como `Self Signed` para agregar un certificado autofirmado.

   a. Introduzca los siguientes detalles:

Opción	Descripción
Nombre común	Especifique el nombre completo del sitio. Para que el sitio se considere de confianza, esta entrada debe coincidir con el nombre de host que introdujo el cliente en el navegador.
Algoritmo	Seleccione EC (criptografía de curva elíptica) o RSA. Se recomienda la opción EC.
Tamaño de clave	Seleccione el nivel de cifrado que se utilizará para los protocolos de enlace: ■ `SECP256R1` se utiliza para los certificados EC. ■ Se recomienda la opción de 2048 bits para los certificados RSA.

   b. En **Nombre alternativo del asunto (SAN)**, haga clic en **Agregar**.

   c Introduzca la dirección IP o el FQDN del clúster, o ambos, de NSX Advanced Load Balancer Controller si se implementa como un solo nodo. Si solo se utiliza la dirección IP o el FQDN, debe coincidir con la dirección IP de la máquina virtual de NSX Advanced Load Balancer Controller que especifique durante la implementación.

   Consulte Implementación de NSX Advanced Load Balancer Controller. Introduzca la dirección IP o el FQDN del clúster de NSX Advanced Load Balancer Controller si se implementa como un clúster de tres nodos.

   d Haga clic en **Guardar**.

   Necesitará este certificado cuando configure el Supervisor para habilitar la funcionalidad de administración de cargas de trabajo.

6 Descargue el certificado autofirmado que creó.

   a Seleccione **Seguridad > Certificados SSL/TLS**.

   Si no ve el certificado, actualice la página.

   b Seleccione el certificado que creó y haga clic en el icono de descarga.

   c En la página **Exportar certificado** que aparece, haga clic en la opción **Copiar en el portapapeles** del certificado. No copie la clave.

   d Guarde el certificado copiado para usarlo más adelante cuando habilite la administración de cargas de trabajo.

7 Si tiene un certificado válido creado previamente, para cargarlo seleccione **Tipo** como `Import`.

   a En **Certificado**, haga clic en **Cargar archivo** e importe el certificado.

   El campo SAN del certificado que cargue debe tener la dirección IP o el FQDN del clúster del controlador.

   Nota Asegúrese de cargar o pegar el contenido del certificado solo una vez.

   b En **Clave (PEM) o PKCS12**, haga clic en **Cargar archivo** e importe la clave.

   c Haga clic en **Validar** para validar el certificado y la clave.

   d Haga clic en **Guardar**.

8 Para cambiar el certificado, realice los siguientes pasos.

   a En el panel de control Controlador, seleccione **Administración > Configuración del sistema**.

   b Haga clic en **Editar**.

   c Seleccione la pestaña **Acceso**.

   d En **Certificado SSL/TLS**, elimine los certificados del portal predeterminados existentes.

   e En el menú desplegable, seleccione el certificado creado o cargado recientemente.

f Seleccione **Autenticación básica**.

g Haga clic en **GUARDAR**.

Limitaciones al usar NSX Advanced Load Balancer

Es importante tener en cuenta las advertencias al configurar NSX Advanced Load Balancer en el entorno de vSphere IaaS control plane.

Una entrada no obtiene una dirección IP externa de NSX Advanced Load Balancer en los siguientes casos:

- Si no se especifica un nombre de host en la configuración de entrada.
- Si la entrada se configura con la opción de configuración `defaultBackend` en lugar del nombre de host.

De forma predeterminada, un recurso de entrada en Kubernetes debe definir el nombre de host en la configuración del controlador para asignarle una IP externa. Esto es necesario porque NSX Advanced Load Balancer utiliza alojamiento virtual para el tráfico en los servicios virtuales que se crean correspondientes a las entradas de Kubernetes. Para obtener más información sobre la opción de configuración `defaultBackend`, consulte https://kubernetes.io/docs/concepts/services-networking/ingress/#default-backend.

Si una entrada tiene el mismo nombre de host que una entrada en un espacio de nombres diferente, no obtiene una dirección IP externa de NSX Advanced Load Balancer. De forma predeterminada, NSX Advanced Load Balancer asigna una VIP única para cada espacio de nombres, lo que significa que todas las entradas en un mismo espacio de nombres comparten la misma VIP. Por lo tanto, dos entradas de espacios de nombres diferentes se asignan a VIP distintas. Sin embargo, si tienen el mismo nombre de host, el servidor DNS no sabe en qué dirección IP debe resolver el nombre de host.

Instalar y configurar el NSX Advanced Load Balancer

Si utiliza redes de vSphere Distributed Switch (vDS), puede instalar y configurar NSX Advanced Load Balancer 22.1.4 en su entorno de vSphere IaaS control plane.

- Compruebe que el entorno cumpla con los requisitos para configurar vSphere IaaS control plane con NSX Advanced Load Balancer. Consulte Requisitos para un supervisor de tres zonas con NSX Advanced Load Balancer y Requisitos para habilitar un supervisor de clúster único con NSX Advanced Load Balancer en *Planificación y conceptos del plano de control de IaaS de vSphere*.

- Descargue el OVA de NSX Advanced Load Balancer. VMware proporciona un archivo OVA de NSX Advanced Load Balancer para que lo implemente en el entorno de vSphere en el que habilitará la administración de cargas de trabajo. Descargue la versión más reciente del archivo OVA compatible con vSphere IaaS control plane desde el portal de VMware Customer Connect.

Nota Los procedimientos descritos en esta guía son relevantes para NSX Advanced Load Balancer, que es compatible con vSphere IaaS control plane 8.0 Update 2. Puede haber disponibles versiones posteriores de NSX Advanced Load Balancer, y los flujos de trabajo de la interfaz de usuario podrían ser diferentes.

Para obtener más información sobre NSX Advanced Load Balancer, consulte la Documentación de VMware NSX Advanced Load Balancer.

Qué leer a continuación

Procedimiento

1 Crear una instancia de vSphere Distributed Switch para un Supervisor para su uso con NSX Advanced Load Balancer

Para configurar un clúster de vSphere como un Supervisor que utiliza la pila de redes de vSphere y NSX Advanced Load Balancer, debe crear una instancia de vSphere Distributed Switch. Cree grupos de puertos en el conmutador distribuido que puede configurar como redes de cargas de trabajo en Supervisor. NSX Advanced Load Balancer necesita un grupo de puertos distribuidos para conectar las interfaces de datos del motor de servicio. El grupo de puertos se utiliza para poner las IP virtuales (VIP) de la aplicación en los motores de servicio.

2 Importar el archivo OVA de NSX Advanced Load Balancer en una biblioteca de contenido local

Para almacenar la imagen OVA de NSX Advanced Load Balancer, cree una biblioteca de contenido local e importe la imagen en ella.

3 Implementar el controlador de NSX Advanced Load Balancer

Implemente la máquina virtual del controlador de NSX Advanced Load Balancer en la red de administración de su entorno de vSphere IaaS control plane.

4 Configurar un grupo de motores de servicio

vSphere IaaS control plane utiliza el grupo de motores de servicio **Grupo predeterminado**. Opcionalmente, puede configurar los motores de servicio **Grupo predeterminado** dentro de un grupo que defina la colocación y el número de máquinas virtuales de motores de servicio en vCenter. También puede configurar la alta disponibilidad si el controlador de NSX Advanced Load Balancer está en modo Enterprise. vSphere IaaS control plane solo admite el motor de servicio **Grupo predeterminado**. No puede crear otros grupos de motores de servicio.

Crear una instancia de vSphere Distributed Switch para un Supervisor para su uso con NSX Advanced Load Balancer

Para configurar un clúster de vSphere como un Supervisor que utiliza la pila de redes de vSphere y NSX Advanced Load Balancer, debe crear una instancia de vSphere Distributed Switch. Cree grupos de puertos en el conmutador distribuido que puede configurar como redes de cargas de trabajo en Supervisor. NSX Advanced Load Balancer necesita un grupo de puertos distribuidos para conectar las interfaces de datos del motor de servicio. El grupo de puertos se utiliza para poner las IP virtuales (VIP) de la aplicación en los motores de servicio.

Requisitos previos

Revise los requisitos del sistema y las topologías de red para usar las redes de vSphere para el Supervisor con NSX Advanced Load Balancer. Consulte Requisitos para un supervisor de tres zonas con NSX Advanced Load Balancer y Requisitos para habilitar un supervisor de clúster único con NSX Advanced Load Balancer en *Planificación y conceptos del plano de control de IaaS de vSphere*.

Procedimiento

1 En vSphere Client, desplácese hasta un centro de datos.

2 Haga clic con el botón derecho en el centro de datos y seleccione **Conmutador distribuido > Nuevo conmutador distribuido**.

3 Escriba un nombre para el conmutador, por ejemplo, **`Conmutador distribuido de cargas de trabajo`**, y haga clic en **Siguiente**.

4 Seleccione la versión 8.0 para el conmutador y haga clic en **Siguiente**.

5 En **Nombre del grupo de puertos**, introduzca **`Red de cargas de trabajo principal`**, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

   Se creará un conmutador distribuido nuevo con un grupo de puertos en el centro de datos. Este grupo de puertos se podrá utilizar como la red de cargas de trabajo principal de la instancia de Supervisor que creará. La red de cargas de trabajo principal controla el tráfico de las máquinas virtuales del plano de control de Kubernetes.

6 Cree grupos de puertos distribuidos para las redes de cargas de trabajo.

   La cantidad de grupos de puertos que cree dependerá de la topología que desee implementar para Supervisor. Para una topología con una red de cargas de trabajo aislada, cree un grupo de puertos distribuidos que se utilizará como red para todos los espacios de nombres en Supervisor. En el caso de una topología con redes aisladas para cada espacio de nombres, cree la misma cantidad de grupos de puertos que de los espacios de nombres que creará.

   a Vaya al conmutador distribuido que se acaba de crear.

   b Haga clic con el botón derecho en el conmutador y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

c Escriba un nombre para el grupo de puertos, por ejemplo, **`Red de cargas de trabajo`**, y haga clic en **Siguiente**.

d Deje los valores predeterminados, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

7 Cree un grupo de puertos para la red de datos .

a Haga clic con el botón derecho en el conmutador distribuido y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

b Escriba un nombre para el grupo de puertos, por ejemplo, **`Red de datos`**, y haga clic en **Siguiente**.

c En la página **Configurar parámetros**, introduzca las propiedades generales del nuevo grupo de puertos distribuidos y haga clic en **Siguiente**.

Propiedad	Descripción
Enlace de puertos	Elija cuándo se deben asignar los puertos a las máquinas virtuales conectadas a este grupo de puertos distribuidos. Seleccione **Enlace estático** para asignar un puerto a una máquina virtual cuando la máquina virtual se conecta al grupo de puertos distribuidos.
Asignación de puertos	Seleccione la asignación de puertos **Elástico**. El número predeterminado de puertos es ocho. Cuando se asignan todos los puertos, se crea un nuevo conjunto de ocho puertos.
Cantidad de puertos	Conserve el valor predeterminado .
Grupo de recursos de red	En el menú desplegable, asigne el nuevo grupo de puertos distribuidos a un grupo de recursos de red definido por el usuario . Si no creó un grupo de recursos de red, el menú está vacío.
VLAN	En el menú desplegable, seleccione el tipo de filtrado y marcado del tráfico de VLAN: ■ **Ninguna**: no utilice la VLAN. Seleccione esta opción si utiliza el etiquetado de conmutador externo . ■ **VLAN**: en el cuadro de texto ID de VLAN, escriba un valor de 1 a 4094 para el etiquetado de conmutador virtual. ■ **Enlace troncal de VLAN**: utilice esta opción para el etiquetado de invitado virtual y para pasar el tráfico de VLAN con un identificador al SO invitado. Escriba un rango troncal de VLAN. Puede configurar varios rangos o VLAN individuales con una lista separada por comas. Por ejemplo, `1702-1705`, `1848-1849`. ■ **VLAN privada**: asocie el tráfico a una VLAN privada creada en el conmutador distribuido. Si no creó ninguna VLAN privada, este menú estará vacío.
Avanzado	Deje esta opción sin seleccionar.

8 En la página **Listo para finalizar**, revise la configuración y haga clic en **Finalizar**.

Resultados

Se crea el conmutador distribuido y los grupos de puertos distribuidos aparecen en el conmutador distribuido. Ahora podrá utilizar este grupo de puertos que creó como la **Red de datos** de NSX Advanced Load Balancer.

Importar el archivo OVA de NSX Advanced Load Balancer en una biblioteca de contenido local

Para almacenar la imagen OVA de NSX Advanced Load Balancer, cree una biblioteca de contenido local e importe la imagen en ella.

La creación de una biblioteca de contenido local implica configurar la biblioteca, descargar los archivos OVA e importarlos a la biblioteca de contenido local. Para obtener más información, consulte Usar bibliotecas de contenido.

Requisitos previos

Compruebe que descargó el archivo OVA de NSX Advanced Load Balancer.

Cree una biblioteca de contenido local. Consulte Crear y editar una biblioteca de contenido.

Procedimiento

1. Inicie sesión en vCenter Server mediante vSphere Client.
2. Seleccione **Menú > Bibliotecas de contenido**.
3. En la lista de **Bibliotecas de contenido**, haga clic en el vínculo del nombre de la biblioteca de contenido local que haya creado. Por ejemplo, **NSX ALB**.
4. Haga clic en **Acciones**.
5. Seleccione **Importar elemento**.
6. En la ventana **Importar elemento de biblioteca**, seleccione **Archivo local**.
7. Haga clic en **Cargar archivos**.
8. Seleccione el archivo OVA que descargó.
9. Haga clic en **Importar**.
10. Despliegue el panel **Tareas recientes** en la parte inferior de la página.
11. Supervise la tarea **Obtener contenido de un elemento de biblioteca** y compruebe que se haya **Completado** correctamente.

Pasos siguientes

Implemente el controlador de NSX Advanced Load Balancer. Consulte Implementar el controlador de NSX Advanced Load Balancer.

Implementar el controlador de NSX Advanced Load Balancer

Implemente la máquina virtual del controlador de NSX Advanced Load Balancer en la red de administración de su entorno de vSphere IaaS control plane.

Requisitos previos

- Compruebe que tiene una red de administración en la que implementar NSX Advanced Load Balancer. Puede ser una instancia de vSphere Distributed Switch (vDS) o un conmutador estándar de vSphere (vSS).
- Compruebe que creó un conmutador vDS y un grupo de puertos para la red de datos. Consulte Crear una instancia de vSphere Distributed Switch para un Supervisor para su uso con NSX Advanced Load Balancer.
- Asegúrese de haber completado los requisitos previos. Consulte Requisitos para un supervisor de tres zonas con NSX Advanced Load Balancer y Requisitos para habilitar un supervisor de clúster único con NSX Advanced Load Balancer en *Planificación y conceptos del plano de control de IaaS de vSphere*.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione el clúster de vSphere designado para los componentes de administración.

3 Cree un grupo de recursos denominado **`AVI-LB`**.

4 Haga clic con el botón derecho en el grupo de recursos y seleccione **Implementar plantilla de OVF**.

5 Seleccione **Archivo local** y haga clic en **Cargar archivos**.

6 Busque y seleccione el archivo `controller-`*`VERSION`*`.ova` que descargó como requisito previo.

7 Introduzca un nombre y seleccione una carpeta para la controladora.

Opción	Descripción
Nombre de la máquina virtual	**`avi-controller-1`**
Ubicación de la máquina virtual	**Centro de datos**

8 Seleccione el grupo de recursos **`AVI-LB`** como recurso informático.

9 Revise los detalles de la configuración y haga clic en **Siguiente**.

10 Seleccione una **Directiva de almacenamiento de máquina virtual**, como **`vsanDatastore`**.

11 Seleccione la red de administración, por ejemplo, **`red-1`**.

12 Personalice la configuración de la siguiente manera y haga clic **Siguiente** cuando haya terminado.

Opción	Descripción
Dirección IP de la interfaz de administración	Introduzca la dirección IP de la máquina virtual del controlador, como `10.199.17.51`.
Máscara de subred de la interfaz de administración	Introduzca la máscara de subred, como `255.255.255.0`.
Puerta de enlace predeterminada	Introduzca la puerta de enlace predeterminada para la red de administración, como `10.199.17.235`.
Clave de autenticación de inicio de sesión de Sysadmim	Opcionalmente pegue el contenido de una clave pública. Puede dejar la clave en blanco.
Nombre de host del Controlador AVI.	Introduzca el FQDN o la dirección IP del controlador.

13 Revise la configuración de implementación.

14 Haga clic en **Finalizar** para completar la configuración.

15 Utilice vSphere Client para supervisar el aprovisionamiento de la máquina virtual del controlador en el panel **Tareas**.

16 Utilice vSphere Client para encender la máquina virtual del controlador después de implementarla.

Implementar un clúster de controladores

De forma opcional, puede implementar un clúster de tres nodos de controlador. Se recomienda configurar un clúster en entornos de producción para HA y recuperación ante desastres. Si va a ejecutar un controlador de NSX Advanced Load Balancer de un solo nodo, deberá utilizar la función Copia de seguridad y restauración.

Para ejecutar un clúster de tres nodos, después de implementar la primera máquina virtual del controlador, implemente y encienda dos máquinas virtuales del controlador adicionales. No debe ejecutar el asistente de configuración inicial ni cambiar la contraseña de administrador de estos controladores . La configuración de la primera máquina virtual del controlador se asigna a las dos nuevas máquinas virtuales del controlador.

Procedimiento

1 Vaya a **Administración > Controlador**.

2 Seleccione **Nodos**.

3 Haga clic en el icono de edición.

4 Agregue una IP estática para **IP del clúster del controlador**.

Esta dirección IP debe ser de la red de administración .

5 En **Nodos del clúster**, configure los dos nuevos nodos de clúster.

Opción	Descripción
IP	Dirección IP del nodo del controlador .
Nombre	Nombre del nodo. El nombre puede ser la dirección IP .
Contraseña	Contraseña del nodo de controlador . Deje la contraseña vacía.
Dirección IP pública	La dirección IP pública del nodo del controlador . Deje esto vacío.

6 Haga clic en **Guardar**.

Nota Una vez que implemente un clúster, deberá usar la IP del clúster del controlador para cualquier configuración adicional y no la IP del nodo del controlador.

Encender el controlador

Después de implementar la máquina virtual del controlador, podrá encenderla. Durante el proceso de arranque, la dirección IP especificada durante la implementación se asigna a la máquina virtual.

Después de encenderlo, el primer proceso de arranque de la máquina virtual del controlador puede tardar hasta 10 minutos.

Requisitos previos

Implemente el controlador.

Procedimiento

1 En vCenter Server, haga clic con el botón derecho en la máquina virtual `avi-controller-1` que implementó.

2 Seleccione **Encender > Encender**.

A la máquina virtual se le asigna la dirección IP que especificó durante la implementación.

3 Para comprobar si la máquina virtual está encendida, acceda a la dirección IP en un navegador.

Cuando la máquina virtual se conecta, aparecen advertencias sobre el certificado TLS y la conexión.

4 En la advertencia **Esta conexión no es privada**, haga clic en **Mostrar detalles**.

5 Haga clic en **Visitar este sitio web** en la ventana que aparece.

Se le solicitarán las credenciales de usuario.

Configurar el controlador

Configure la máquina virtual del controlador para su entorno de vSphere IaaS control plane y configure una nube.

Para conectar el plano de control del equilibrador de carga con el entorno de vCenter Server, el controlador requiere varios parámetros de configuración posteriores a la implementación. Durante la configuración inicial del controlador, se crea una nube de Nube predeterminada en la que se implementa el primer controlador. Para permitir que el equilibrador de carga pueda atender varias instancias de vCenter Center o varios centros de datos, puede crear nubes personalizadas de tipo VMware vCenter para cada combinación de vCenter y centro de datos. Para obtener más información, consulte Componentes de NSX Advanced Load Balancer.

Requisitos previos

- Compruebe que el entorno cumpla con los requisitos del sistema para configurar NSX Advanced Load Balancer. Consulte Requisitos para un supervisor de tres zonas con NSX Advanced Load Balancer y Requisitos para habilitar un supervisor de clúster único con NSX Advanced Load Balancer en *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Implemente el controlador.

Procedimiento

1 Con un explorador, diríjase a la dirección IP que especificó al implementar el controlador.

2 Cree una **Cuenta de administrador**.

Opción	Descripción
Nombre de usuario	El nombre de usuario del administrador para la configuración inicial. No puede editar este campo.
Contraseña	Introduzca una contraseña de administrador para la máquina virtual del controlador. La contraseña debe tener al menos 8 caracteres y contener una combinación de caracteres numéricos, caracteres especiales, mayúsculas y minúsculas.
Confirmar contraseña	Vuelva a introducir la contraseña del administrador.
Dirección de correo electrónico (opcional)	Introduzca una dirección de correo electrónico del administrador. Se recomienda proporcionar una dirección de correo electrónico para recuperar la contraseña en un entorno de producción.

3 Ajuste **Configuración del sistema**.

Opción	Descripción
Frase de contraseña	Introduzca una frase de contraseña para la copia de seguridad del controlador. Se realiza una copia de seguridad automática de la configuración del controlador en el disco local de forma periódica. Para obtener más información, consulte Copia de seguridad y restauración. La frase de contraseña debe tener al menos 8 caracteres y contener una combinación de caracteres numéricos, caracteres especiales, mayúsculas y minúsculas.
Confirmar frase de contraseña	Vuelva a introducir la frase de contraseña de copia de seguridad.

Opción	Descripción
Resolutor de DNS	Introduzca una dirección IP para el servidor DNS que está utilizando en el entorno de vSphere IaaS control plane. Por ejemplo, `10.14.7.12`.
Dominios de búsqueda de DNS	Introduzca una cadena de dominio.

4 (opcional) Configure los ajustes de **Correo electrónico/SMTP**.

Opción	Descripción
Origen de SMTP	Seleccione una de las siguientes opciones **Ninguno**, **Host local**, **Servidor SMTP** o **Servidor anónimo**. El valor predeterminado es **Host local**.
Dirección de remitente	La dirección de correo electrónico.

5 Haga clic en **Siguiente**.

6 Configure los ajustes de varios tenants.

  a Conserve el acceso de tenant predeterminado.

  b Seleccione **Configurar nube después de** y haga clic en **Guardar**.

  Nota Si no seleccionó la opción **Configurar nube después de** antes de guardar, se cierra el asistente de configuración inicial. La ventana de configuración de la nube no se inicia automáticamente y se le dirige a una vista de panel de control en el controlador. En este caso, desplácese hasta **Infraestructura > Nubes** y configure la nube.

7 Configure la nube de **VMware vCenter/vSphere ESX**. Haga clic en **Crear** y **VMware vCenter/vSphere ESX** como tipo de nube.

  Aparecerá la página de configuración de **NUEVA NUBE**.

8 Configure los ajustes de la sección **General**.

Opción	Descripción
Nombre	Introduzca un nombre para la nube. Por ejemplo, **`Nube predeterminada`**.
Tipo	El tipo de nube es **VMware vCenter/vSphere ESX**.

9 (opcional) En la sección **Administración de direcciones IP de red predeterminada**, seleccione **DHCP habilitado** si DHCP está disponible en los grupos de puertos vSphere.

  Deje la opción sin seleccionar si desea que las interfaces del motor de servicio utilicen solo direcciones IP estáticas. Puede configurarlos individualmente para cada red.

  Para obtener más información, consulte Configurar una red IP virtual.

10 Configure las opciones de **Configuración de ubicación de servicios virtuales**.

Opción	Descripción
Preferir rutas estáticas frente a redes conectadas directamente para la ubicación de servicios virtuales	Seleccione esta opción para forzar que la máquina virtual del motor de servicio acceda a la red del servidor mediante el enrutamiento a través de la puerta de enlace predeterminada. De forma predeterminada, el controlador conecta directamente una NIC a la red del servidor, por lo que debe forzar al motor de servicio a conectarse solo a la red de datos y enrutarse a la red de carga de trabajo.
Usar rutas estáticas para la resolución de red de VIP	Deje esta opción sin seleccionar.

11 Configure las credenciales de **vCenter/vSphere**.

Haga clic en **Establecer credenciales** e introduzca los siguientes detalles:

Opción	Descripción
Dirección de vCenter	Escriba el nombre de host o la dirección IP de vCenter Server para el entorno de vSphere IaaS control plane.
Nombre de usuario	Introduzca el nombre de usuario del administrador de vCenter, como administrator@vsphere.local. Para usar permisos menores, cree una función dedicada. Consulte Función de usuario de VMware para obtener más información.
Contraseña	Introduzca la contraseña de usuario.
Permisos de acceso	**Lectura**: cree y administre las máquinas virtuales del motor de servicios. **Escritura**: el controlador crea y administra las máquinas virtuales del motor de servicios. Debe seleccionar Escritura.

12 Configure los ajustes del **Centro de datos**.

a Seleccione el **centro de datos** de vSphere donde desea habilitar **Administración de cargas de trabajo**.

b Seleccione la opción **Usar biblioteca de contenido** y seleccione la biblioteca de contenido local en la lista.

13 Seleccione **GUARDAR Y REINICIAR** para crear la nube **VMware vCenter/vSphere ESX** con los ajustes que configuró.

14 Configure los ajustes de **Red**.

Opción	Descripción
Red de administración	Seleccione la red de máquina virtual. Los motores de servicio utilizarán esta interfaz de red para conectarse con el controlador.
Motor de servicio	Deje la plantilla **Grupo de motores de servicio** vacía.
Administración de dirección IP de red de administración:	Seleccione **DHCP habilitado**.

15 (opcional) Configure los siguientes ajustes de red solo si no selecciona **DHCP habilitado**.

Opción	Descripción
Subred IP	Introduzca la subred IP para la red de administración. Por ejemplo, `10.199.32.0/24`. **Nota** Introduzca una subred IP solo si DHCP no está disponible.
Puerta de enlace predeterminada	Introduzca la puerta de enlace predeterminada de la red de administración, como `10.199.32.253`. **Nota** Introduzca una subred IP solo si DHCP no está disponible.
Agregar grupo de direcciones IP estáticas	Introduzca una o más direcciones IP o rangos de direcciones IP. Por ejemplo, `10.99.32.62-10.199.32.65`. **Nota** Introduzca una subred IP solo si DHCP no está disponible.

16 Cree un perfil de IPAM y configure los ajustes de **IPAM/DNS**.

Se requiere IPAM para asignar direcciones IP virtuales cuando se crean servicios virtuales.

a En el menú Más acciones de **Perfil IPAM**, seleccione **Crear**.

Se mostrará la página **NUEVO PERFIL IPAM/DNS**.

b Configure el **Perfil de IPAM**.

Opción	Descripción
Nombre	Cadena definida por el usuario, como **`ipam-profile`**
Tipo	Seleccione **AVI Vantage IPAM**
Asignar IP en VRF	Anule la selección de esta opción.
Nube	Seleccione **Nube personalizada** en la lista desplegable.

c Haga clic en **Agregar** en la **Red utilizable** y seleccione la red IP virtual que configuró. Esta red es la red principal.

d Haga clic en **GUARDAR**.

17 (opcional) Configure los ajustes de NTP si desea utilizar un servidor NTP interno.

a Seleccione **Administración > Configuración > DNS/NTP**.

b Elimine los servidores NTP existentes, si los hubiera, e introduzca la dirección IP del servidor DNS que está utilizando. Por ejemplo, `192.168.100.1`.

Resultados

Una vez completada la configuración, verá **panel de control** del controlador. Seleccione **Infraestructura > Nubes** y compruebe que el estado del controlador de **Nube personalizada** sea de color verde. A veces, el estado puede ser amarillo durante algún tiempo hasta que la Controladora detecte todos los grupos de puertos en el entorno de vCenter Server, antes de que cambie a verde.

Agregar una licencia

Cuando haya configurado NSX Advanced Load Balancer, deberá asignarle una licencia. El controlador arranca en modo de evaluación, que dispone de todas las funciones equivalentes a las de una licencia de edición Enterprise. Debe asignar una licencia válida de nivel Enterprise al controlador antes de que caduque su período de evaluación.

Requisitos previos

Compruebe que dispone de la licencia de nivel Enterprise.

Procedimiento

1 En el panel de control Controladora de NSX Advanced Load Balancer, seleccione **Administración > Licencias**.

2 Seleccione **Configuración**.

3 Seleccione **Nivel Enterprise**

4 Haga clic en **GUARDAR**.

5 Para agregar la licencia, seleccione **Cargar desde equipo**.

   Después de cargar el archivo de licencia, aparece en la lista de licencias del controlador. El sistema muestra la información sobre la licencia, incluidas la fecha de inicio y la fecha de caducidad.

Asignar un certificado al controlador

El controlador debe enviar un certificado a los clientes para establecer una comunicación segura. Este certificado debe tener un **Nombre alternativo del asunto (SAN)** que coincida con el nombre de host o la dirección IP del clúster del controlador NSX Advanced Load Balancer.

El controlador tiene un certificado autofirmado predeterminado. Sin embargo, este certificado no tiene el SAN correcto. Debe reemplazarlo por un certificado válido o autofirmado que tenga el SAN correcto. Puede crear un certificado autofirmado o cargar un certificado externo.

Para obtener más información sobre los certificados, consulte la documentación de AVI.

Procedimiento

1 En el panel de control Controlador, haga clic en el menú de la esquina superior izquierda y seleccione **Plantillas > Seguridad**.

2 Seleccione **Certificados SSL/TLS**.

3 Para crear un certificado, haga clic en **Crear** y seleccione **Certificado de controlador**.

   Aparecerá la ventana **Nuevo certificado (SSL/TLS)**.

4 Introduzca un nombre para el certificado.

5 Si no tiene un certificado válido creado previamente, seleccione **Tipo** como `Self Signed` para agregar un certificado autofirmado.

   a Introduzca los siguientes detalles:

Opción	Descripción
Nombre común	Especifique el nombre completo del sitio. Para que el sitio se considere de confianza, esta entrada debe coincidir con el nombre de host que introdujo el cliente en el navegador.
Algoritmo	Seleccione EC (criptografía de curva elíptica) o RSA. Se recomienda la opción EC.
Tamaño de clave	Seleccione el nivel de cifrado que se utilizará para los protocolos de enlace: ■ `SECP256R1` se utiliza para los certificados EC. ■ Se recomienda la opción de 2048 bits para los certificados RSA.

   b En **Nombre alternativo del asunto (SAN)**, haga clic en **Agregar**.

   c Introduzca la dirección IP o el FQDN del clúster, o ambos, del controlador AVI si se implementa como un solo nodo. Si solo se utiliza la dirección IP o el FQDN, debe coincidir con la dirección IP de la máquina virtual del controlador que especifique durante la implementación.

   Consulte Implementar el controlador de NSX Advanced Load Balancer.

   Introduzca la dirección IP o el FQDN del clúster del controlador de NSX Advanced Load Balancer si se implementa como un clúster de tres nodos. Para obtener información sobre la implementación de un clúster de tres nodos de controlador, consulte Implementar un clúster de controladores.

   d Haga clic en **Guardar**.

   Necesitará este certificado cuando configure el Supervisor para habilitar la funcionalidad de administración de cargas de trabajo.

6 Descargue el certificado autofirmado que creó.

   a Seleccione **Seguridad > Certificados SSL/TLS**.

   Si no ve el certificado, actualice la página.

   b Seleccione el certificado que creó y haga clic en el icono de descarga.

   c En la página **Exportar certificado** que aparece, haga clic en la opción **Copiar en el portapapeles** del certificado. No copie la clave.

   d Guarde el certificado copiado para usarlo más adelante cuando habilite la administración de cargas de trabajo.

7 Si tiene un certificado válido creado previamente, para cargarlo seleccione **Tipo** como `Import`.

   a En **Certificado**, haga clic en **Cargar archivo** e importe el certificado.

      El campo SAN del certificado que cargue debe tener la dirección IP o el FQDN del clúster del controlador.

      Nota Asegúrese de cargar o pegar el contenido del certificado solo una vez.

   b En **Clave (PEM) o PKCS12**, haga clic en **Cargar archivo** e importe la clave.

   c Haga clic en **Validar** para validar el certificado y la clave.

   d Haga clic en **Guardar**.

8 Para cambiar el certificado del portal, realice los siguientes pasos.

   a En el panel de control Controlador, seleccione **Administración > Configuración del sistema**.

   b Haga clic en **Editar**.

   c Seleccione la pestaña **Acceso**.

   d En **Certificado SSL/TLS**, elimine los certificados del portal predeterminados existentes.

   e En el menú desplegable, seleccione el certificado creado o cargado recientemente.

   f Seleccione **Autenticación básica**.

   g Haga clic en **GUARDAR**.

Configurar un grupo de motores de servicio

vSphere IaaS control plane utiliza el grupo de motores de servicio **Grupo predeterminado**. Opcionalmente, puede configurar los motores de servicio **Grupo predeterminado** dentro de un grupo que defina la colocación y el número de máquinas virtuales de motores de servicio en vCenter. También puede configurar la alta disponibilidad si el controlador de NSX Advanced Load Balancer está en modo Enterprise. vSphere IaaS control plane solo admite el motor de servicio **Grupo predeterminado**. No puede crear otros grupos de motores de servicio.

Para obtener información sobre cómo aprovisionar la capacidad sobrante en caso de una conmutación por error, consulte la documentación de AVI.

Procedimiento

1 En el panel Controladora de NSX Advanced Load Balancer, seleccione **Infraestructura > Recursos de nube > Grupo de motores de servicio**.

2 En la página **Grupo de motores de servicio**, haga clic en el icono Editar en **Grupo predeterminado**.

   Aparecerá la pestaña **Ajustes generales**.

   vSphere IaaS control plane solo admite **Nube predeterminada**.

3 En la sección **Colocación**, seleccione el **Modo de alta disponibilidad**.

La opción predeterminada es `N + M (buffer)`. Puede mantener el valor predeterminado o seleccionar una de las siguientes opciones:

- `Active/Standy`
- `Active/Active`

4 En la sección **Motor de servicio**, puede configurar el exceso de capacidad para el grupo motor de servicio.

La opción **Número de motores de servicio** define el número máximo de motores de servicio que se pueden crear dentro de un grupo de motores de servicio. El valor predeterminado es **10**.

Para configurar el exceso de capacidad, especifique un valor en **Motores de servicio del búfer**. El valor que especifique es la cantidad de máquinas virtuales que se implementan para garantizar un exceso de capacidad en caso de una conmutación por error.

El valor predeterminado es **1**.

5 En la sección **Servicio virtual**, configure las siguientes opciones.

Opción	Descripción
Servicios virtuales por motor de servicio	La cantidad máxima de servicios virtuales que el clúster del controlador puede colocar en cualquiera de los motores de servicio del grupo. Introduzca un valor de **1000**.
Colocación de servicios virtuales en los motores de servicio	Seleccione **Distribuido**. Al seleccionar esta opción, se maximiza el rendimiento mediante la colocación de servicios virtuales en los motores de servicio recién encendidos hasta la cantidad máxima de motores de servicio especificados. El valor predeterminado es **Compacto**.

6 Puede mantener los valores predeterminados para los demás ajustes.

7 Haga clic en **Guardar**.

Configurar rutas estáticas

Una puerta de enlace predeterminada permite al motor de servicio enrutar el tráfico a los servidores de grupo en la red de cargas de trabajo. Debe configurar la dirección IP de puerta de enlace de la red de datos como la puerta de enlace predeterminada . Los motores de servicio no obtienen la IP de puerta de enlace predeterminada de DHCP en las redes de datos. Debe configurar rutas estáticas para que los motores de servicio puedan enrutar el tráfico a las redes de carga de trabajo y la IP del cliente correctamente.

Procedimiento

1 En el panel de control Controladora de NSX Advanced Load Balancer, seleccione **Infraestructura > Recursos de nube > Contexto VRF**.

2 Haga clic en **Crear**.

3 En la configuración **General**, introduzca un nombre para el contexto de enrutamiento.

4 En la sección **Ruta estática**, haga clic en **AGREGAR**.

5 En **Subred de puerta de enlace**, introduzca `172.16.10.0/24`.

6 En **Salto siguiente**, introduzca la dirección IP de puerta de enlace para la red de datos.

   Por ejemplo, `192.168.1.1`.

7 (opcional) Seleccione **Emparejamiento de BGP** para configurar los detalles locales y del mismo nivel de BGP.

   Para obtener más información, consulte la documentación de Avi.

8 Haga clic en **Guardar**.

Configurar una red IP virtual

Configure una subred IP virtual (VIP) para la red de datos. Puede configurar el rango de VIP que se utilizará cuando se ponga un servicio virtual en la red VIP específica. Puede configurar DHCP para los motores de servicio. Opcionalmente, si DHCP no está disponible, puede configurar un grupo de direcciones IP que se asignarán a la interfaz del motor de servicio de esa red. vSphere IaaS control plane solo admite una red VIP.

Procedimiento

1 En el panel de control Controlador de NSX Advanced Load Balancer, **Infraestructura > Recursos de nube > Redes**.

2 Seleccione la nube de la lista.

   Por ejemplo, seleccione **Nube predeterminada**.

3 Introduzca un nombre para la red.

   Por ejemplo, `Data Nework`.

4 Mantenga **DHCP habilitado** seleccionado si DHCP está disponible en la red de datos.

   Anule la selección de esta opción si DHCP no está disponible.

5 Seleccione **Activar configuración automática de IPv6**.

   La Controladora de NSX Advanced Load Balancer detecta el CIDR de red automáticamente si una máquina virtual se está ejecutando en la red y aparece con el tipo **Detectado**.

6 Si la Controladora de NSX Advanced Load Balancer detecta la subred IP automáticamente, configure el rango de IP de la subred.

   a Edite la configuración.

   b Introduzca un **Prefijo de subred**.

   c Si DHCP está disponible para la dirección IP del motor de servicio, anule la selección de **Usar dirección IP estática para VIP y SE**.

d Introduzca una o varias direcciones IP o rangos de direcciones IP.

Por ejemplo, `10.202.35.1-10.202.35.254`.

Nota Puede introducir una dirección IP que termine con `0`. Por ejemplo, `192.168.0.0` y omita cualquier advertencia que aparezca.

e Haga clic en **Guardar**.

7 Si el controlador no detecta una subred IP y su tipo, realice los siguientes pasos:

a Haga clic en **Agregar**.

b Introduzca un **Prefijo de subred**.

c Haga clic en **AGREGAR**.

d Si DHCP está disponible para la dirección IP del motor de servicio, anule la selección de **Usar dirección IP estática para VIP y SE**.

e En **Dirección IP**, introduzca el CIDR de la red que proporciona las direcciones IP virtuales.

Por ejemplo, `10.202.35.0/22`

f Introduzca una o varias direcciones IP o rangos de direcciones IP.

El rango debe ser un subconjunto del CIDR de red en **Subred IP**. Por ejemplo, `10.202.35.1-10.202.35.254`.

Nota Puede introducir una dirección IP que termine con `0`. Por ejemplo, `192.168.0.0` y omita cualquier advertencia que aparezca.

g Haga clic en **Guardar** para guardar la configuración de subred.

La **Red** muestra la subred IP con el tipo **Configurado** y un grupo de direcciones IP.

8 Haga clic en **Guardar** para guardar la configuración de red.

Resultados

La página **Red** muestra las redes configuradas.

Ejemplo

La red `Primary Workload Network` muestra la red detectada como `10.202.32.0/22` y las subredes configuradas como `10.202.32.0/22 [254/254]`. Esto indica que 254 direcciones IP virtuales provienen de `10.202.32.0/22`. Tenga en cuenta que la vista de resumen no muestra los rangos de IP `10.202.35.1-10.202.35.254`.

Probar el NSX Advanced Load Balancer

Después de implementar y configurar el plano control de NSX Advanced Load Balancer, compruebe su funcionalidad.

Procedimiento

1 En el panel de la controladora de AVI, vaya a **Infraestructura (Infrastructure) > Nubes (Clouds)**.

2 Compruebe que el estado de la controladora de **Nube predeterminada (Default-Cloud)** esté de color verde.

   Para solucionar los problemas que podría encontrar, consulte Recopilar paquetes de soporte para la solución de problemas de NSX Advanced Load Balancer.

Instalar y configurar el equilibrador de carga de HAProxy

VMware proporciona una implementación del equilibrador de carga de HAProxy de código abierto que se puede usar en el entorno de vSphere IaaS control plane. Si utiliza redes de vSphere Distributed Switch (vDS) para la **administración de cargas de trabajo**, puede instalar y configurar el equilibrador de carga de HAProxy.

Crear una instancia de vSphere Distributed Switch para un Supervisor para su uso con el equilibrador de carga de HAProxy

Para configurar un clúster de vSphere como un Supervisor que utiliza la pila de redes de vSphere y el equilibrador de carga de HAProxy, debe agregar los hosts a una instancia de vSphere Distributed Switch. Debe crear grupos de puertos en el conmutador distribuido que configurará como redes de cargas de trabajo en el Supervisor.

Puede seleccionar entre diferentes topologías para Supervisor en función del nivel de aislamiento que desee proporcionar a las cargas de trabajo de Kubernetes que se ejecutarán en el clúster.

Requisitos previos

- Revise los requisitos del sistema para usar redes de vSphere para el Supervisor con el equilibrador de carga de HAProxy. Consulte Requisitos para habilitar un supervisor de tres zonas con el equilibrador de carga de HAProxy y Requisitos para habilitar un supervisor de clúster único con redes de VDS y el equilibrador de carga de HAProxy *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Determine la topología para configurar redes de cargas de trabajo con HAProxy en el Supervisor. Consulte Topologías para implementar el equilibrador de carga de HAProxy en *Planificación y conceptos del plano de control de IaaS de vSphere*.

Procedimiento

1 En vSphere Client, desplácese hasta un centro de datos.

2 Haga clic con el botón derecho en el centro de datos y seleccione **Conmutador distribuido > Nuevo conmutador distribuido**.

3 Escriba un nombre para el conmutador, por ejemplo, **`Conmutador distribuido de cargas de trabajo`**, y haga clic en **Siguiente**.

4 Seleccione la versión 7.0 para el conmutador y haga clic en **Siguiente**.

5 En **Nombre del grupo de puertos**, introduzca `Red de cargas de trabajo principal`, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

   Se creará un conmutador distribuido nuevo con un grupo de puertos en el centro de datos. Este grupo de puertos se podrá utilizar como la red de cargas de trabajo principal de la instancia de Supervisor que creará. La red de cargas de trabajo principal controla el tráfico de las máquinas virtuales del plano de control de Kubernetes.

6 Cree grupos de puertos distribuidos para las redes de cargas de trabajo.

   La cantidad de grupos de puertos que cree dependerá de la topología que desee implementar para Supervisor. Para una topología con una red de cargas de trabajo aislada, cree un grupo de puertos distribuidos que se utilizará como red para todos los espacios de nombres en Supervisor. En el caso de una topología con redes aisladas para cada espacio de nombres, cree la misma cantidad de grupos de puertos que de los espacios de nombres que creará.

   a Vaya al conmutador distribuido que se acaba de crear.

   b Haga clic con el botón derecho en el conmutador y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

   c Escriba un nombre para el grupo de puertos, por ejemplo, `Red de cargas de trabajo`, y haga clic en **Siguiente**.

   d Deje los valores predeterminados, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

7 Agregue los hosts de los clústeres de vSphere que vaya a configurar como Supervisor en el conmutador distribuido.

   a Haga clic con el botón derecho en el conmutador distribuido y seleccione **Agregar y administrar hosts**.

   b Seleccione **Agregar hosts**.

   c Haga clic en **Nuevos hosts**, seleccione los hosts del clúster de vSphere que vaya a configurar como Supervisor y haga clic en **Siguiente**.

   d Seleccione una NIC física de cada host y asígnele un vínculo superior en el conmutador distribuido.

   e Haga clic en **Siguiente** en las pantallas del asistente que irán apareciendo y, por último, haga clic en **Finalizar**.

Resultados

Se agregarán los hosts al conmutador distribuido. Ahora podrá utilizar los grupos de puertos que cree en el conmutador como redes de cargas de trabajo de Supervisor.

Implementar la máquina virtual del plano de control del equilibrador de carga de HAProxy

Si desea utilizar la pila de redes de vSphere para cargas de trabajo de Kubernetes, instale la máquina virtual del plano de control de HAProxy para proporcionar servicios de equilibrio de carga a los clústeres de Tanzu Kubernetes.

Requisitos previos

- Compruebe que el entorno cumpla con los requisitos informáticos y de red para implementar HAProxy. Consulte Requisitos para habilitar un supervisor de tres zonas con el equilibrador de carga de HAProxy y Requisitos para habilitar un supervisor de clúster único con redes de VDS y el equilibrador de carga de HAProxy *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Compruebe si tiene una red de administración en el conmutador estándar o distribuido de vSphere en el que se va a implementar el equilibrador de carga de HAProxy. El Supervisor se comunica con el equilibrador de carga de HAProxy en esa red de administración.
- Cree una instancia de vSphere Distributed Switch y grupos de puertos para redes de cargas de trabajo. El equilibrador de carga de HAProxy se comunica con los nodos del Supervisor y del clúster de Tanzu Kubernetes a través de las redes de cargas de trabajo. Consulte Crear una instancia de vSphere Distributed Switch para un Supervisor para su uso con el equilibrador de carga de HAProxy. Para obtener información sobre las redes de cargas de trabajo, consulte Redes de cargas de trabajo en el clúster supervisor en *Planificación y conceptos del plano de control de IaaS de vSphere*.
- Descargue la versión más reciente del archivo OVA de VMware HAProxy desde el sitio de VMware-HAProxy.
- Seleccione una topología para implementar el equilibrador de carga de HAProxy y las redes de cargas de trabajo en el Supervisor. Consulte Topologías para implementar el equilibrador de carga de HAProxy en *Planificación y conceptos del plano de control de IaaS de vSphere*.

Le puede resultar útil ver una demostración de cómo se utiliza vSphere IaaS control plane con las redes de vDS y HAProxy. Vea el vídeo Introducción al uso de vSphere with Tanzu.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Cree una máquina virtual nueva a partir del archivo OVA de HAProxy.

Opción	Descripción
Biblioteca de contenido	Si importó el archivo OVA a una biblioteca de contenido local: ■ Vaya a **Menú > Biblioteca de contenido**. ■ Seleccione la biblioteca en la que importó el archivo OVA. ■ Seleccione la plantilla `vmware-haproxy-vX.X.X`. ■ Haga clic con el botón derecho y elija **Nueva máquina virtual desde esta plantilla**.
Archivo local	Si descargó el archivo OVA en el host local: ■ Seleccione el clúster de vCenter en el que se habilitará **Administración de cargas de trabajo**. ■ Haga clic con el botón derecho y seleccione **Implementar plantilla de OVF**. ■ Seleccione **Archivo local** y haga clic en **Cargar archivos**. ■ Desplácese hasta el archivo `vmware-haproxy-vX.X.X.ova` y selecciónelo.

3 Introduzca un valor en **Nombre de la máquina virtual**, como **`haproxy`**.

4 Seleccione el **centro de datos** donde va a implementar HAProxy y haga clic en **Siguiente**.

5 Seleccione el clúster de vCenter en el que se habilitará **Administración de cargas de trabajo** y haga clic en **Siguiente**.

6 Revise y confirme los detalles de la implementación y haga clic en **Siguiente**.

7 Acepte los acuerdos de licencia y haga clic en **Siguiente**.

8 Seleccione una configuración de implementación. Consulte Topología de red de HAProxy en *Planificación y conceptos del plano de control de IaaS de vSphere* para obtener detalles.

Configuración	Descripción
Predeterminado	Seleccione esta opción para implementar el dispositivo con 2 NIC: una red de administración y una sola red de cargas de trabajo.
Red de front-end	Seleccione esta opción para implementar el dispositivo con 3 NIC. La subred de front-end se utiliza para aislar los nodos del clúster de la red que utilizan los desarrolladores para acceder al plano de control del clúster.

9 Seleccione la política de almacenamiento que se utilizará para la máquina virtual y haga clic en **Siguiente**.

10 Seleccione las interfaces de red que se utilizarán para el equilibrador de carga y haga clic en **Siguiente**.

Red de origen	Red de destino
Administración	Seleccione la red de administración, como `Red de máquinas virtuales`.
Carga de trabajo	Seleccione el grupo de puertos de vDS configurado para **Administración de cargas de trabajo**.
Front-end	Seleccione el grupo de puertos de vDS configurado para la subred de front-end. Si no seleccionó la configuración de front-end, esta opción se ignorará durante la instalación, por lo que puede dejar el valor predeterminado.

Nota La red de carga de trabajo debe estar en una subred diferente a la red de administración. Consulte Requisitos para habilitar un supervisor de tres zonas con el equilibrador de carga de HAProxy y Requisitos para habilitar un supervisor de clúster único con redes de VDS y el equilibrador de carga de HAProxy *Planificación y conceptos del plano de control de IaaS de vSphere*.

11 Personalice los ajustes de configuración de la aplicación. Consulte Ajustes de configuración del dispositivo.

12 Proporcione los detalles de configuración de red. Consulte Configuración de red.

13 Configure el equilibrio de carga. Consulte Configuración del equilibrio de carga.

14 Haga clic en **Siguiente** para completar la configuración del archivo OVA.

15 Revise los detalles de configuración de la implementación y haga clic en **Finalizar** para implementar el archivo OVA.

16 Supervise la implementación de la máquina virtual mediante el panel de **tareas**.

17 Cuando finalice la implementación de la máquina virtual, enciéndala.

Pasos siguientes

Una vez que el equilibrador de carga de HAProxy se implemente y se encienda correctamente, continúe con la habilitación de **Administración de cargas de trabajo**. Consulte Capítulo 12 Configurar y administrar un Supervisor.

Personalizar el equilibrador de carga de HAProxy

Personalice la máquina virtual del plano de control de HAProxy, incluidos los ajustes de configuración, la configuración de red y la configuración del equilibrio de carga.

Ajustes de configuración del dispositivo

En la tabla se enumeran y describen los parámetros para configurar el dispositivo de HAProxy.

Parámetro	Descripción	Observación o ejemplo
Contraseña raíz	Contraseña inicial del usuario raíz (6-128 caracteres).	Los cambios subsiguientes de contraseña deben realizarse en el sistema operativo.
Permitir inicio de sesión de usuario raíz	Opción para permitir que el usuario raíz inicie sesión en la máquina virtual de forma remota a través de SSH.	El inicio de sesión de usuario raíz puede ser necesario para solucionar problemas, pero tenga en cuenta las implicaciones de seguridad al conceder este permiso.
Entidad de certificación TLS (ca.crt)	Para utilizar el certificado de CA autofirmado, deje este campo vacío. Para utilizar su propio certificado de CA (ca.crt), pegue su contenido en este campo. Es posible que tenga que codificar el contenido en Base64. https://www.base64encode.org/	Si utiliza el certificado de CA autofirmado, las claves pública y privada se generarán a partir del certificado.
Clave (ca.key)	Si utiliza el certificado autofirmado, deje este campo vacío. Si proporcionó un certificado de CA, pegue el contenido de la clave privada del certificado en este campo.	

Configuración de red

En la tabla se enumeran y describen los parámetros para configurar la red de HAProxy.

Parámetro	Descripción	Observación o ejemplo
Nombre del host	El nombre de host (o FQDN) que se asignará a la máquina virtual del plano de control de HAProxy.	Valor predeterminado: `haproxy.local`
DNS	Una lista separada por comas de direcciones IP del servidor DNS.	Valores predeterminados: `1.1.1.1, 1.0.0.1` Valor de ejemplo: `10.8.8.8`
IP de gestión	La dirección IP estática de la máquina virtual del plano de control de HAProxy en la red de administración.	Una dirección IPv4 válida con la longitud de prefijo de la red; por ejemplo: `192.168.0.2/24`.
Puerta de enlace de administración	La dirección IP de la puerta de enlace para la red de administración.	Por ejemplo: `192.168.0.1`
IP de carga de trabajo	La dirección IP estática de la máquina virtual del plano de control de HAProxy en la red de cargas de trabajo. Esta dirección IP debe estar fuera del rango de direcciones IP del equilibrador de carga.	Una dirección IPv4 válida con la longitud de prefijo de la red; por ejemplo: `192.168.10.2/24`.

Parámetro	Descripción	Observación o ejemplo
Puerta de enlace de carga de trabajo	La dirección IP de la puerta de enlace para la red de cargas de trabajo.	Por ejemplo: `192.168.10.1` Si selecciona la configuración de front-end, debe introducir una puerta de enlace. La implementación no se realizará correctamente si se selecciona el front-end y no se especifica ninguna puerta de enlace.
IP de front-end	La dirección IP estática del dispositivo de HAProxy en la red de front-end. Este valor solo se utiliza cuando se selecciona el modelo de implementación de front-end.	Una dirección IPv4 válida con la longitud de prefijo de la red; por ejemplo: `192.168.100.2/24`
Puerta de enlace de front-end	La dirección IP de la puerta de enlace para la red de front-end. Este valor solo se utiliza cuando se selecciona el modelo de implementación de front-end.	Por ejemplo: `192.168.100.1`

Configuración del equilibrio de carga

En la tabla se enumeran y describen los parámetros para configurar el equilibrador de carga de HAProxy.

Parámetro	Descripción	Ejemplo u observación
Rango(s) de direcciones IP del equilibrador de carga	En este campo se especifica un rango de direcciones IPv4 con el formato CIDR. El valor debe ser un rango de CIDR válido o se producirá un error en la instalación. HAProxy reserva las direcciones IP para las direcciones IP virtuales (VIP). Una vez que se asignan, se asignará cada dirección VIP y HAProxy responderá a las solicitudes en esa dirección. El rango de CIDR que se especifique aquí no deberá superponerse con las direcciones IP que se asignen para los servidores virtuales cuando se habilite **Administración de cargas de trabajo** en vCenter Server mediante vSphere Client. **Nota** El rango de direcciones IP del equilibrador de carga debe estar en una subred diferente a la red de administración. No es posible tener el rango de IP del equilibrador de carga en la misma subred que la red de administración.	Por ejemplo, el CIDR de red `192.168.100.0/24` proporciona las 256 direcciones IP virtuales del equilibrador de carga con el rango `192.168.100.0 - 192.168.100.255`. Por ejemplo, el CIDR de red `192.168.100.0/25` proporciona las 128 direcciones IP virtuales del equilibrador de carga con el rango `192.168.100.0 - 192.168.100.127`.
Puerto de administración de la API del plano de datos	El puerto de la máquina virtual de HAProxy en el que escucha el servicio de API del equilibrador de carga.	Un puerto válido. El puerto 22 se reserva para SSH. El valor predeterminado es `5556`.
ID de usuario de HAProxy	Nombre de usuario de la API del equilibrador de carga	El nombre de usuario que utilizan los clientes para autenticarse en el servicio de API del equilibrador de carga. **Nota** Necesita este nombre de usuario cuando habilite Supervisor.
Contraseña de HAProxy	Contraseña de la API del equilibrador de carga	La contraseña que utilizan los clientes para autenticarse en el servicio de API del equilibrador de carga. **Nota** Necesita esta contraseña cuando habilite el Supervisor.

Implementar Supervisor de tres zonas

5

Implemente Supervisor en tres zonas de vSphere para obtener alta disponibilidad en el nivel de clúster. Cada zona de vSphere se asigna a un clúster de vSphere.

Nota Si actualizó el entorno de vSphere IaaS control plane de una versión de vSphere anterior a la 8.0 y desea utilizar zonas de vSphere para las implementaciones, como los clústeres de Tanzu Kubernetes Grid, debe crear un nuevo Supervisor de tres zonas.

Lea los siguientes temas a continuación:

- Implementar un Supervisor de tres zonas con la pila de redes de VDS
- Implementar un Supervisor de tres zonas con redes de NSX

Implementar un Supervisor de tres zonas con la pila de redes de VDS

Consulte cómo implementar un Supervisor con la pila de redes VDS en tres zonas de vSphere. Cada zona de vSphere se asigna a un clúster de vSphere. Al implementar Supervisor en tres zonas de vSphere, se brinda alta disponibilidad a las cargas de trabajo en el nivel del clúster. Supervisor configurado con redes de VDS admite clústeres y máquinas virtuales de Tanzu Kubernetes Grid creadas a través del servicio de máquina virtual. No admite pods de vSphere.

Requisitos previos

- Complete los requisitos previos para configurar clústeres de vSphere como un Supervisor. Consulte Requisitos previos para configurar vSphere IaaS control plane en clústeres de vSphere.
- Cree tres zonas de vSphere. Consulte Capítulo 3 Crear zonas de vSphere para una implementación de Supervisor de varias zonas.

Procedimiento

1 En el menú de inicio, seleccione **Administración de cargas de trabajo**.

2 Seleccione una opción de licencias para Supervisor.

   - Si tiene una licencia de Tanzu Edition válida, haga clic en **Agregar licencia** para agregar la clave de licencia al inventario de licencias de vSphere.

- Si aún no tiene una licencia de Tanzu Edition, introduzca los detalles de contacto para poder recibir la comunicación de VMware y haga clic en **Comenzar**.

El período de evaluación de Supervisor dura 60 días. Dentro de ese período, debe asignar una licencia válida de Tanzu Edition al clúster. Si agregó una clave de licencia de Tanzu Edition, podrá asignar esa misma clave en el período de evaluación de 60 días una vez que haya completado la configuración de Supervisor.

3 En la pantalla **Administración de cargas de trabajo**, haga clic de nuevo en **Comenzar**.

4 Seleccione la página **vCenter Server y red** y el sistema vCenter Server que se configuró para la implementación de Supervisor. A continuación, seleccione **vSphere Distributed Switch (VDS)** como pila de redes y haga clic en **Siguiente**.

5 En la página **Ubicación de supervisor**, seleccione **Implementación de zona de vSphere** para implementar un Supervisor en tres zonas de vSphere.

   a Introduzca un nombre para el nuevo Supervisor.

   b Seleccione el centro de datos en el que creó las zonas de vSphere para implementar el Supervisor.

   c En la lista de zonas de vSphere compatibles, seleccione tres zonas.

   d Haga clic en **Siguiente**.

6 En la página **Almacenamiento**, configure el almacenamiento para la colocación de máquinas virtuales del plano de control.

Opción	Descripción
Nodo del plano de control	Seleccione la directiva de almacenamiento para la colocación de las máquinas virtuales del plano de control.

7 En la pantalla **Equilibrador de carga**, configure los ajustes de un equilibrador de carga.

a Introduzca un nombre para el equilibrador de carga.

b Seleccione el tipo de equilibrador de carga.

Puede seleccionar entre **NSX Advanced Load Balancer** y **HAProxy**.

c Configurar los ajustes del equilibrador de carga

- Introduzca la siguiente configuración para NSX Advanced Load Balancer:

Opción	Descripción
Nombre	Introduzca un nombre para NSX Advanced Load Balancer.
Endpoint de la controladora de NSX Advanced Load Balancer	Dirección IP del controlador de NSX Advanced Load Balancer. El puerto predeterminado es `443`.
Nombre de usuario	El nombre de usuario que está configurado con NSX Advanced Load Balancer. Utilice este nombre de usuario para acceder al controlador.
Contraseña	La contraseña para el nombre de usuario.
Certificado de servidor	El certificado utilizado por el controlador. Puede proporcionar el certificado que asignó durante la configuración. Para obtener más información, consulte Asignar un certificado al controlador.
Nombre de nube	Introduzca el nombre de la nube personalizada que configuró. Tenga en cuenta que el nombre de la nube distingue entre mayúsculas y minúsculas. Para utilizar **Default-Cloud**, deje este campo vacío. Para obtener más información, consulte Configurar el controlador.

- Introduzca la siguiente configuración para HAProxy:

Opción	Descripción
Endpoint de la controladora de equilibrador de carga de HAProxy	La dirección IP y el puerto de la API del plano de datos de HAProxy, que es la dirección IP de administración del dispositivo de HAProxy. Este componente controla el servidor de HAProxy y se ejecuta dentro de la máquina virtual de HAProxy.
Nombre de usuario	El nombre de usuario que está configurado con el archivo OVA de HAProxy. Este nombre se utiliza para autenticarse con la API del plano de datos de HAProxy.
Contraseña	La contraseña para el nombre de usuario.

<table>
<tr><th>Opción</th><th>Descripción</th></tr>
<tr><td>Rangos de direcciones IP virtuales</td><td>El rango de direcciones IP que utilizan los clústeres de Tanzu Kubernetes en la red de cargas de trabajo. Este rango de IP proviene de la lista de direcciones IP que se definieron en el CIDR que configuró durante la implementación del dispositivo de HAProxy. Puede establecer todo el rango configurado en la implementación de HAProxy, pero también puede establecer un subconjunto de ese CIDR si desea crear varios Supervisores y utilizar direcciones IP de ese rango de CIDR. Este rango no debe superponerse con el rango de IP definido para la red de cargas de trabajo en este asistente. El rango tampoco debe superponerse con ningún ámbito DHCP en esta red de cargas de trabajo.</td></tr>
<tr><td>Certificado TLS de administración de HAProxy</td><td>El certificado en formato PEM que está firmado o es una raíz de confianza del certificado de servidor que presenta la API del plano de datos.

Opción 1: Si se habilita el acceso raíz, ejecute SSH en la máquina virtual de HAProxy como usuario raíz y copie <code>/etc/haproxy/ca.crt</code> en la Entidad de certificación de servidor. No utilice líneas de escape con el formato <code>\n</code>.
Opción 2: Haga clic con el botón derecho en la máquina virtual de HAProxy y seleccione Editar configuración. Copie el certificado de CA desde el campo correspondiente y conviértalo desde Base64 mediante una herramienta de conversión como https://www.base64decode.org/.
Opción 3: Ejecute el siguiente script de PowerCLI. Reemplace las variables <code>$vc</code>, <code>$vc_user</code> y <code>$vc_password</code> con los valores correspondientes.
<pre>
$vc = "10.21.32.43"
$vc_user =
"administrator@vsphere.local"
$vc_password = "PASSWORD"
Connect-VIServer -User $vc_user
-Password $vc_password -Server $vc
$VMname = "haproxy-demo"
$AdvancedSettingName =
"guestinfo.dataplaneapi.cacert"
$Base64cert = get-vm $VMname |Get-
AdvancedSetting -Name
$AdvancedSettingName
while
([string]::IsNullOrEmpty($Base64cert
.Value)) {
     Write-Host "Waiting for CA
Cert Generation... This may take a
under 5-10
minutes as the VM needs to boot and
generate the CA Cert
</pre>
</td></tr>
</table>

Opción	Descripción
	`(if you haven't provided one already)."` ` $Base64cert = get-vm $VMname	Get-AdvancedSetting -Name $AdvancedSettingName` ` Start-sleep -seconds 2` ` }` ` Write-Host "CA Cert Found... Converting from BASE64"` ` $cert = [Text.Encoding]::Utf8.GetString([Convert]::FromBase64String($Base64cert.Value))` `Write-Host $cert`

8 En la pantalla **Red de administración**, configure los parámetros de la red que se utilizarán para las máquinas virtuales del plano de control de Kubernetes.

a Seleccione un **Modo de red**.

- **Red DHCP**. En este modo, todas las direcciones IP de la red de administración, como las direcciones IP de las máquinas virtuales del plano de control, una dirección IP flotante, los servidores DNS, DNS, los dominios de búsqueda y el servidor NTP, se adquieren automáticamente desde un servidor DHCP. Para obtener direcciones IP flotantes, el servidor DHCP debe estar configurado para admitir identificadores de cliente. En el modo DHCP, todas las máquinas virtuales del plano de control utilizan identificadores de cliente DHCP estables para adquirir direcciones IP. Estos identificadores de cliente se pueden utilizar para configurar la asignación de direcciones IP estáticas para que las direcciones IP de las máquinas virtuales del plano de control en el servidor DHCP se aseguren de que no cambien. No se admite el cambio de las direcciones IP de las máquinas virtuales del plano de control ni las direcciones IP flotantes.

  Es posible anular algunos de los ajustes heredados de DHCP. Para ello, introduzca valores en los campos de texto de estos ajustes.

Opción	Descripción
Red	Seleccione la red que controlará el tráfico de administración para el Supervisor
IP flotante	Introduzca una dirección IP que determine el punto de inicio para reservar cinco direcciones IP consecutivas para las máquinas virtuales del plano de control de Kubernetes de la siguiente manera: ■ Una dirección IP para cada una de las máquinas virtuales del plano de control de Kubernetes. ■ Una dirección IP flotante para una de las máquinas virtuales del plano de control de Kubernetes a la que se prestará servicio como una interfaz a la red de administración. La máquina virtual del plano de control que tiene asignada la dirección IP flotante actúa como una máquina virtual principal para las tres máquinas virtuales del plano de control de Kubernetes. La dirección IP flotante se traslada al nodo del plano de control que es el líder de etcd en este clúster de Kubernetes. Esto mejora la disponibilidad en el caso de un evento de partición de red. ■ Una dirección IP que se va a utilizar como búfer en caso de que una máquina virtual de plano de control de Kubernetes falle y se ponga en marcha una nueva máquina virtual de plano de control para reemplazarla.

Opción	Descripción
Servidores DNS	Introduzca las direcciones de los servidores DNS que utiliza en su entorno. Si el sistema vCenter Server está registrado con un FQDN, debe introducir las direcciones IP de los servidores DNS que utiliza con el entorno de vSphere para que el FQDN se pueda resolver en el Supervisor.
Dominios de búsqueda DNS	Introduzca los nombres de dominio que DNS busca dentro de los nodos del plano de control de Kubernetes, como `corp.local`, para que el servidor DNS pueda resolverlos.
Servidores NTP	Introduzca las direcciones de los servidores NTP que utiliza en su entorno, si los hubiera.

- **Estático**. Introduzca manualmente toda la configuración de red de la red de administración.

Opción	Descripción
Red	Seleccione la red que controlará el tráfico de administración para el Supervisor
Dirección IP inicial	Introduzca una dirección IP que determine el punto de inicio para reservar cinco direcciones IP consecutivas para las máquinas virtuales del plano de control de Kubernetes de la siguiente manera: ■ Una dirección IP para cada una de las máquinas virtuales del plano de control de Kubernetes. ■ Una dirección IP flotante para una de las máquinas virtuales del plano de control de Kubernetes a la que se prestará servicio como una interfaz a la red de administración. La máquina virtual del plano de control que tiene asignada la dirección IP flotante actúa como una máquina virtual principal para las tres máquinas virtuales del plano de control de Kubernetes. La dirección IP flotante se traslada al nodo del plano de control que es el líder de etcd en este clúster de Kubernetes. Esto mejora la disponibilidad en el caso de un evento de partición de red. ■ Una dirección IP que se va a utilizar como búfer en caso de que una máquina virtual de plano de control de Kubernetes falle y se ponga en marcha una nueva máquina virtual de plano de control para reemplazarla.
Máscara de subred	Solo se aplica a la configuración de IP estática. Introduzca una máscara de subred para la red de administración. Por ejemplo, `255.255.255.0`

Opción	Descripción
Puerta de enlace	Introduzca una puerta de enlace para la red de administración.
Servidores DNS	Introduzca las direcciones de los servidores DNS que utiliza en su entorno. Si el sistema vCenter Server está registrado con un FQDN, debe introducir las direcciones IP de los servidores DNS que utiliza con el entorno de vSphere para que el FQDN se pueda resolver en el Supervisor.
Dominios de búsqueda DNS	Introduzca los nombres de dominio que DNS busca dentro de los nodos del plano de control de Kubernetes, como `corp.local`, para que el servidor DNS pueda resolverlos.
Servidores NTP	Introduzca las direcciones de los servidores NTP que utiliza en su entorno, si los hubiera.

b Haga clic en **Siguiente**.

9 En la página **Red de carga de trabajo**, introduzca la configuración de la red que controlará el tráfico de red de las cargas de trabajo de Kubernetes que se ejecutan en Supervisor.

Nota Si selecciona el uso de un servidor DHCP para proporcionar la configuración de red para las redes de carga de trabajo, no podrá crear ninguna red de carga de trabajo nueva una vez que complete la configuración del Supervisor.

a Seleccione un modo de red.

- **Red DHCP**. En este modo de red, toda la configuración de red de las redes de carga de trabajo se adquiere a través de DHCP. También es posible anular algunos de los ajustes heredados de DHCP. Para ello, introduzca valores en los campos de texto de estos ajustes:

Opción	Descripción
Red interna para servicios de Kubernetes	Introduzca una anotación de CIDR que determine el rango de direcciones IP para los clústeres y los servicios de Tanzu Kubernetes que se ejecutan dentro de los clústeres.
Grupo de puertos	Seleccione el grupo de puertos que servirá como red de carga de trabajo principal en el Supervisor. La red principal controla el tráfico de las máquinas virtuales del plano de control de Kubernetes y el tráfico de las cargas de trabajo de Kubernetes. En función de la topología de red, podrá asignar más adelante un grupo de puertos diferente que sirva como red para cada espacio de nombres. De esta forma, podrá proporcionar aislamiento de capa 2 entre los espacios de nombres en Supervisor. Los espacios de nombres que no tienen un grupo de puertos diferente asignado como red usan la red principal. Los clústeres de Tanzu Kubernetes solo usan la red que está asignada al espacio de nombres en el que se implementan o bien utilizan la red principal si no hay ninguna red explícita asignada a ese espacio de nombres.
Nombre de red	Introduzca el nombre de la red.
Servidores DNS	Introduzca las direcciones IP de los servidores DNS que utiliza con su entorno, si los hubiera. Por ejemplo, `10.142.7.1`. Cuando se introduce la dirección IP del servidor DNS, se agrega una ruta estática a cada máquina virtual del plano de control. Esto indica que el tráfico a los servidores DNS pasa por la red de cargas de trabajo.

Opción	Descripción
	Si los servidores DNS que especifica se comparten entre la red de administración y la red de cargas de trabajo, las búsquedas de DNS en las máquinas virtuales del plano de control se enrutan a través de la red de cargas de trabajo después de la configuración inicial.
Servidores NTP	Introduzca la dirección del servidor NTP que utiliza con su entorno si existe alguno.

- **Estático**. Configure manualmente los ajustes de la red de carga de trabajo

Opción	Descripción
Red interna para servicios de Kubernetes	Introduzca una anotación de CIDR que determine el rango de direcciones IP para los clústeres y los servicios de Tanzu Kubernetes que se ejecutan dentro de los clústeres.
Grupo de puertos	Seleccione el grupo de puertos que servirá como red de carga de trabajo principal en el Supervisor. La red principal controla el tráfico de las máquinas virtuales del plano de control de Kubernetes y el tráfico de las cargas de trabajo de Kubernetes. En función de la topología de red, podrá asignar más adelante un grupo de puertos diferente que sirva como red para cada espacio de nombres. De esta forma, podrá proporcionar aislamiento de capa 2 entre los espacios de nombres en Supervisor. Los espacios de nombres que no tienen un grupo de puertos diferente asignado como red usan la red principal. Los clústeres de Tanzu Kubernetes solo usan la red que está asignada al espacio de nombres en el que se implementan o bien utilizan la red principal si no hay ninguna red explícita asignada a ese espacio de nombres.
Nombre de red	Introduzca el nombre de la red.
Rangos de direcciones IP	Introduzca un rango de direcciones IP para asignar la dirección IP de las máquinas virtuales y las cargas de trabajo del plano de control de Kubernetes. Este rango de direcciones conecta los nodos del Supervisor y, en el caso de una sola red de cargas de trabajo, también conecta los nodos del clúster de Tanzu Kubernetes. Este rango de direcciones IP no debe superponerse con el rango de VIP del equilibrador de carga cuando se utiliza la configuración **Predeterminado** para HAProxy.
Máscara de subred	Introduzca la dirección IP de la máscara de subred.

Opción	Descripción
Puerta de enlace	Introduzca la puerta de enlace de la red principal.
Servidores NTP	Introduzca la dirección del servidor NTP que utiliza con su entorno si existe alguno.
Servidores DNS	Introduzca las direcciones IP de los servidores DNS que utiliza con su entorno, si los hubiera. Por ejemplo, `10.142.7.1`.

b Haga clic en **Siguiente**.

10 En la página **Revisar y confirmar**, desplácese hacia arriba, revise todos los ajustes que configuró hasta el momento y establezca los ajustes avanzados para la implementación de Supervisor.

Opción	Descripción
Tamaño del plano de control del supervisor	Seleccione el tamaño de las máquinas virtuales del plano de control. El tamaño de las máquinas virtuales del plano de control determina la cantidad de cargas de trabajo que puede ejecutar en Supervisor. Puede elegir lo siguiente: ■ Muy pequeño: 2 CPU, 8 GB de memoria, 32 GB de almacenamiento ■ Pequeño: 4 CPU, 16 GB de memoria, 32 GB de almacenamiento ■ Mediano: 8 CPU, 16 GB de memoria, 32 GB de almacenamiento ■ Grande: 16 CPU, 32 GB de memoria, 32 GB de almacenamiento **Nota** Una vez que seleccione el tamaño del plano de control, solo podrá escalar verticalmente. No podrá escalar horizontalmente a un tamaño menor.
Nombres DNS del servidor de API	De forma opcional, introduzca los FQDN que se utilizarán para acceder al plano de control de Supervisor, en lugar de utilizar la dirección IP del plano de control de Supervisor. Los FQDN que introduzca se integrarán en un certificado generado automáticamente. Al utilizar los FQDN para el Supervisor, puede omitir la especificación de un espacio de IP en el certificado del equilibrador de carga.
Exportar configuración	Exporte un archivo JSON que contenga los valores que introdujo de la configuración de Supervisor. Luego puede modificar e importar el archivo si desea volver a implementar Supervisor o implementar un nuevo Supervisor con una configuración similar. La exportación de la configuración de Supervisor puede ahorrar tiempo porque no se tienen que volver a introducir todos los valores de configuración en este asistente en caso de volver a implementar Supervisor.

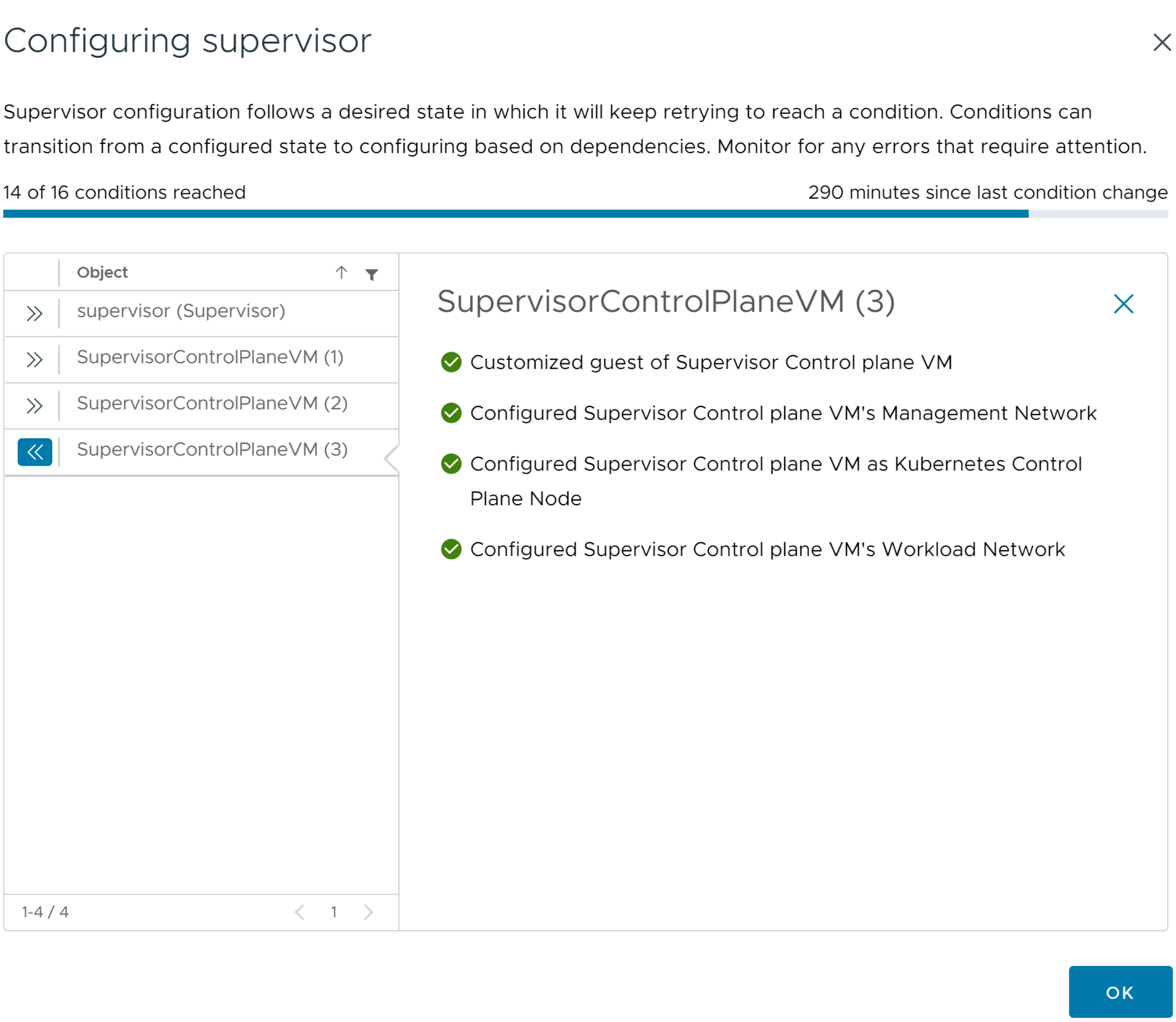
11 Haga clic en **Finalizar** cuando haya terminado de revisar la configuración.

La habilitación del Supervisor inicia la creación y la configuración de las máquinas virtuales del plano de control y otros componentes.

Pasos siguientes

Una vez completado el asistente para habilitar Supervisor, podrá realizar un seguimiento del proceso de activación y observar los posibles problemas que se deban solucionar. En la columna **Estado de configuración**, haga clic en **Ver** junto al estado del Supervisor.

Figura 5-1. Vista de activación del supervisor



Para que se complete el proceso de implementación, el Supervisor debe alcanzar el estado deseado, lo que significa que se cumplen todas las condiciones. Cuando un Supervisor se habilita correctamente, su estado cambia de Configurando a En ejecución. Mientras el Supervisor se encuentra en el estado Configurando, se vuelve a intentar de forma continua alcanzar cada una de las condiciones. Si no se alcanza una condición, se vuelve a intentar la operación hasta que se completa correctamente. Por este motivo, el número de condiciones que se alcanzan puede cambiar una y otra vez, por ejemplo, *10 de 16 condiciones alcanzadas*, luego *4 de 16 condiciones alcanzadas* y así sucesivamente. En casos excepcionales, el estado puede cambiar a Error si existen errores que impiden alcanzar el estado deseado.

Para obtener más información sobre los errores de implementación y la forma de solucionarlos, consulte Resolver los estados de errores en las máquinas virtuales del plano de control de un Supervisor durante una activación o una actualización.

Si desea volver a implementar Supervisor modificando los valores de configuración que introdujo en el asistente, revise Capítulo 9 Implementar un Supervisor mediante la importación de un archivo de configuración JSON.

Implementar un Supervisor de tres zonas con redes de NSX

Consulte cómo implementar un Supervisor con NSX en tres zonas de vSphere. Cada zona de vSphere se asigna a un clúster de vSphere. Al implementar Supervisor en tres zonas de vSphere, se brinda alta disponibilidad a las cargas de trabajo en el nivel del clúster. Un Supervisor de tres zonas configurado con NSX solo admite máquinas virtuales y clústeres de Tanzu Kubernetes; no es compatible con pods de vSphere.

Si configuró la versión 4.1.1 o posterior de NSX e instaló, configuró y registró la versión 22.1.4 o posterior de NSX Advanced Load Balancer con licencia Enterprise en NSX, el equilibrador de carga que se utilizará con NSX es NSX Advanced Load Balancer. Si configuró versiones de NSX anteriores a la 4.1.1, se utilizará el equilibrador de carga de NSX. Para obtener información, consulte Capítulo 7 Comprobar el equilibrador de carga utilizado con redes NSX.

Requisitos previos

- Complete los requisitos previos para configurar clústeres de vSphere como un Supervisor. Consulte Requisitos previos para configurar vSphere IaaS control plane en clústeres de vSphere.
- Cree tres zonas de vSphere. Consulte Capítulo 3 Crear zonas de vSphere para una implementación de Supervisor de varias zonas.

Procedimiento

1. En el menú de inicio, seleccione **Administración de cargas de trabajo**.
2. Seleccione una opción de licencias para Supervisor.
   - Si tiene una licencia de Tanzu Edition válida, haga clic en **Agregar licencia** para agregar la clave de licencia al inventario de licencias de vSphere.
   - Si aún no tiene una licencia de Tanzu Edition, introduzca los detalles de contacto para poder recibir la comunicación de VMware y haga clic en **Comenzar**.

   El período de evaluación de Supervisor dura 60 días. Dentro de ese período, debe asignar una licencia válida de Tanzu Edition al clúster. Si agregó una clave de licencia de Tanzu Edition, podrá asignar esa misma clave en el período de evaluación de 60 días una vez que haya completado la configuración de Supervisor.
3. En la pantalla **Administración de cargas de trabajo**, haga clic de nuevo en **Comenzar**.

4 En la página **vCenter Server y red**, seleccione el sistema vCenter Server que se configuró para la implementación del Supervisor y seleccione **NSX** como pila de redes.

5 Haga clic en **Siguiente**.

6 En la página **Ubicación de supervisor**, seleccione **Implementación de zona de vSphere** para implementar un Supervisor en tres zonas de vSphere.

   a Introduzca un nombre para el nuevo Supervisor.

   b Seleccione el centro de datos en el que creó las zonas de vSphere para implementar el Supervisor.

   c En la lista de zonas de vSphere compatibles, seleccione tres zonas.

   d Haga clic en **Siguiente**.

7 Seleccione directivas de almacenamiento para el Supervisor.

Opción	Descripción
Directiva de almacenamiento del plano de control	Seleccione la directiva de almacenamiento para la colocación de las máquinas virtuales del plano de control.
Directiva de almacenamiento de discos efímeros	Esta opción se encuentra deshabilitada porque los pods de vSphere no son compatibles con un Supervisor de 3 zonas.
Directiva de almacenamiento de caché de imágenes	Esta opción se encuentra deshabilitada porque los pods de vSphere no son compatibles con un Supervisor de 3 zonas.

8 Haga clic en **Siguiente**.

9 En la pantalla **Red de administración**, configure los parámetros de la red que se utilizarán para las máquinas virtuales del plano de control de Kubernetes.

a Seleccione un **Modo de red**.

- **Red DHCP**. En este modo, todas las direcciones IP de la red de administración, como las direcciones IP de las máquinas virtuales del plano de control, una dirección IP flotante, los servidores DNS, DNS, los dominios de búsqueda y el servidor NTP, se adquieren automáticamente desde un servidor DHCP. Para obtener direcciones IP flotantes, el servidor DHCP debe estar configurado para admitir identificadores de cliente. En el modo DHCP, todas las máquinas virtuales del plano de control utilizan identificadores de cliente DHCP estables para adquirir direcciones IP. Estos identificadores de cliente se pueden utilizar para configurar la asignación de direcciones IP estáticas para que las direcciones IP de las máquinas virtuales del plano de control en el servidor DHCP se aseguren de que no cambien. No se admite el cambio de las direcciones IP de las máquinas virtuales del plano de control ni las direcciones IP flotantes.

  Es posible anular algunos de los ajustes heredados de DHCP. Para ello, introduzca valores en los campos de texto de estos ajustes.

Opción	Descripción
Red	Seleccione la red que controlará el tráfico de administración para el Supervisor
IP flotante	Introduzca una dirección IP que determine el punto de inicio para reservar cinco direcciones IP consecutivas para las máquinas virtuales del plano de control de Kubernetes de la siguiente manera: ■ Una dirección IP para cada una de las máquinas virtuales del plano de control de Kubernetes. ■ Una dirección IP flotante para una de las máquinas virtuales del plano de control de Kubernetes a la que se prestará servicio como una interfaz a la red de administración. La máquina virtual del plano de control que tiene asignada la dirección IP flotante actúa como una máquina virtual principal para las tres máquinas virtuales del plano de control de Kubernetes. La dirección IP flotante se traslada al nodo del plano de control que es el líder de etcd en este clúster de Kubernetes. Esto mejora la disponibilidad en el caso de un evento de partición de red. ■ Una dirección IP que se va a utilizar como búfer en caso de que una máquina virtual de plano de control de Kubernetes falle y se ponga en marcha una nueva máquina virtual de plano de control para reemplazarla.

Opción	Descripción
Servidores DNS	Introduzca las direcciones de los servidores DNS que utiliza en su entorno. Si el sistema vCenter Server está registrado con un FQDN, debe introducir las direcciones IP de los servidores DNS que utiliza con el entorno de vSphere para que el FQDN se pueda resolver en el Supervisor.
Dominios de búsqueda DNS	Introduzca los nombres de dominio que DNS busca dentro de los nodos del plano de control de Kubernetes, como `corp.local`, para que el servidor DNS pueda resolverlos.
Servidores NTP	Introduzca las direcciones de los servidores NTP que utiliza en su entorno, si los hubiera.

- **Estático**. Introduzca manualmente toda la configuración de red de la red de administración.

Opción	Descripción
Red	Seleccione la red que controlará el tráfico de administración para el Supervisor
Dirección IP inicial	Introduzca una dirección IP que determine el punto de inicio para reservar cinco direcciones IP consecutivas para las máquinas virtuales del plano de control de Kubernetes de la siguiente manera: ■ Una dirección IP para cada una de las máquinas virtuales del plano de control de Kubernetes. ■ Una dirección IP flotante para una de las máquinas virtuales del plano de control de Kubernetes a la que se prestará servicio como una interfaz a la red de administración. La máquina virtual del plano de control que tiene asignada la dirección IP flotante actúa como una máquina virtual principal para las tres máquinas virtuales del plano de control de Kubernetes. La dirección IP flotante se traslada al nodo del plano de control que es el líder de etcd en este clúster de Kubernetes. Esto mejora la disponibilidad en el caso de un evento de partición de red. ■ Una dirección IP que se va a utilizar como búfer en caso de que una máquina virtual de plano de control de Kubernetes falle y se ponga en marcha una nueva máquina virtual de plano de control para reemplazarla.
Máscara de subred	Solo se aplica a la configuración de IP estática. Introduzca una máscara de subred para la red de administración. Por ejemplo, `255.255.255.0`

Opción	Descripción
Puerta de enlace	Introduzca una puerta de enlace para la red de administración.
Servidores DNS	Introduzca las direcciones de los servidores DNS que utiliza en su entorno. Si el sistema vCenter Server está registrado con un FQDN, debe introducir las direcciones IP de los servidores DNS que utiliza con el entorno de vSphere para que el FQDN se pueda resolver en el Supervisor.
Dominios de búsqueda DNS	Introduzca los nombres de dominio que DNS busca dentro de los nodos del plano de control de Kubernetes, como `corp.local`, para que el servidor DNS pueda resolverlos.
Servidores NTP	Introduzca las direcciones de los servidores NTP que utiliza en su entorno, si los hubiera.

b Haga clic en **Siguiente**.

10 En el panel **Red de cargas de trabajo**, configure las opciones de las redes para los espacios de nombres.

Opción	Descripción
vSphere Distributed Switch	Seleccione la instancia de vSphere Distributed Switch que controla las redes de superposición para Supervisor. Por ejemplo, seleccione `DSwitch`.
servidor DNS	Introduzca las direcciones IP de los servidores DNS que utiliza con su entorno, si los hubiera. Por ejemplo, `10.142.7.1`.
Modo NAT	El modo NAT está seleccionado de forma predeterminada. Si anula la selección de la opción, se podrá acceder directamente a todas las cargas de trabajo, como los pods de vSphere, las máquinas virtuales y las direcciones IP de los nodos de los clústeres de Tanzu Kubernetes desde fuera de la puerta de enlace de nivel 0, y no tendrá que configurar los CIDR de salida. **Nota** Si anula la selección del modo NAT, no se admitirá el almacenamiento de volumen de archivos.
Red de espacio de nombres	Introduzca uno o varios CIDR de IP para crear subredes o segmentos y asignar direcciones IP a las cargas de trabajo.
CIDR de entrada	Introduzca una anotación CIDR que determine el rango de IP de entrada para los servicios de Kubernetes. Este rango se utiliza para los servicios de tipo equilibrador de carga y entrada.
Clúster de Edge	Seleccione el clúster de NSX Edge que tenga la puerta de enlace de nivel 0 que desee utilizar para las redes de espacio de nombres. Por ejemplo, seleccione `EDGE-CLUSTER`.
Puerta de enlace de nivel 0	Seleccione la puerta de enlace de nivel 0 que se asociará con la puerta de enlace de nivel 1 del clúster.

Opción	Descripción
Prefijo de subred	Introduzca el prefijo de subred que especifica el tamaño de la subred reservada para los segmentos de espacios de nombres. El valor predeterminado es 28.
CIDR de servicio	Introduzca una anotación CIDR para determinar el rango de IP de los servicios de Kubernetes. Puede utilizar el valor predeterminado.
CIDR de egreso	Introduzca una anotación CIDR que determine la IP de salida de los servicios de Kubernetes. Solo se asigna una dirección IP de egreso para cada espacio de nombres en el Supervisor. La IP de salida es la dirección IP que las cargas de trabajo de Kubernetes en el espacio de nombres concreto utilizan para comunicarse fuera de NSX.

11 Haga clic en **Siguiente**.

12 En la página **Revisar y confirmar**, desplácese hacia arriba, revise todos los ajustes que configuró hasta el momento y establezca los ajustes avanzados para la implementación de Supervisor.

Opción	Descripción
Tamaño del plano de control del supervisor	Seleccione el tamaño de las máquinas virtuales del plano de control. El tamaño de las máquinas virtuales del plano de control determina la cantidad de cargas de trabajo que puede ejecutar en Supervisor. Puede elegir lo siguiente: ■ Muy pequeño: 2 CPU, 8 GB de memoria, 32 GB de almacenamiento ■ Pequeño: 4 CPU, 16 GB de memoria, 32 GB de almacenamiento ■ Mediano: 8 CPU, 16 GB de memoria, 32 GB de almacenamiento ■ Grande: 16 CPU, 32 GB de memoria, 32 GB de almacenamiento **Nota** Una vez que seleccione el tamaño del plano de control, solo podrá escalar verticalmente. No podrá escalar horizontalmente a un tamaño menor.
Nombres DNS del servidor de API	De forma opcional, introduzca los FQDN que se utilizarán para acceder al plano de control de Supervisor, en lugar de utilizar la dirección IP del plano de control de Supervisor. Los FQDN que introduzca se integrarán en un certificado generado automáticamente. Al utilizar los FQDN para el Supervisor, puede omitir la especificación de un espacio de IP en el certificado del equilibrador de carga.
Exportar configuración	Exporte un archivo JSON que contenga los valores que introdujo de la configuración de Supervisor. Luego puede modificar e importar el archivo si desea volver a implementar Supervisor o implementar un nuevo Supervisor con una configuración similar. La exportación de la configuración de Supervisor puede ahorrar tiempo porque no se tienen que volver a introducir todos los valores de configuración en este asistente en caso de volver a implementar Supervisor.

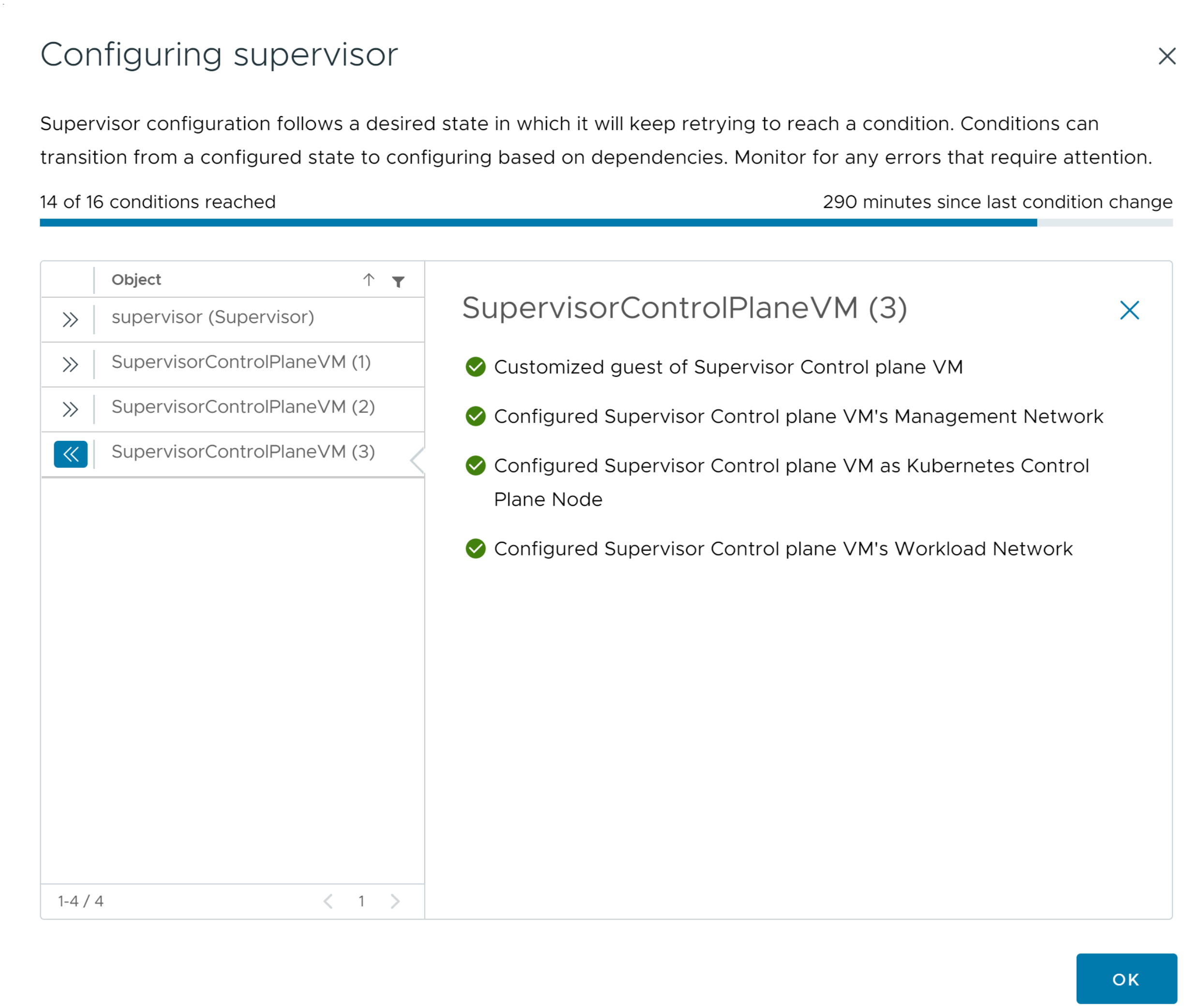
13 Haga clic en **Finalizar** cuando haya terminado de revisar la configuración.

La habilitación del Supervisor inicia la creación y la configuración de las máquinas virtuales del plano de control y otros componentes.

Pasos siguientes

Una vez completado el asistente para habilitar Supervisor, podrá realizar un seguimiento del proceso de activación y observar los posibles problemas que se deban solucionar. En la columna **Estado de configuración**, haga clic en **Ver** junto al estado del Supervisor.

Figura 5-2. Vista de activación del supervisor



Para que se complete el proceso de implementación, el Supervisor debe alcanzar el estado deseado, lo que significa que se cumplen todas las condiciones. Cuando un Supervisor se habilita correctamente, su estado cambia de Configurando a En ejecución. Mientras el Supervisor se encuentra en el estado Configurando, se vuelve a intentar de forma continua alcanzar cada una de las condiciones. Si no se alcanza una condición, se vuelve a intentar la operación hasta que se completa correctamente. Por este motivo, el número de condiciones que se alcanzan puede cambiar una y otra vez, por ejemplo, *10 de 16 condiciones alcanzadas*, luego *4 de 16 condiciones alcanzadas* y así sucesivamente. En casos excepcionales, el estado puede cambiar a Error si existen errores que impiden alcanzar el estado deseado.

Para obtener más información sobre los errores de implementación y la forma de solucionarlos, consulte Resolver los estados de errores en las máquinas virtuales del plano de control de un Supervisor durante una activación o una actualización.

Si desea volver a implementar Supervisor modificando los valores de configuración que introdujo en el asistente, revise Capítulo 9 Implementar un Supervisor mediante la importación de un archivo de configuración JSON.

Implementar un Supervisor de una sola zona

6

Implemente un Supervisor en un clúster de vSphere que se asigne automáticamente a una zona de vSphere. Un Supervisor de una zona obtiene alta disponibilidad de nivel de host a través de vSphere HA.

Lea los siguientes temas a continuación:

- Implementar un Supervisor de una sola zona con la pila de redes de VDS
- Implementar un Supervisor de zona única con redes de NSX

Implementar un Supervisor de una sola zona con la pila de redes de VDS

Consulte cómo implementar Supervisor de una sola zona con la pila de redes de VDS y con el equilibrador de carga de HA Proxy o NSX Advanced Load Balancer. Un Supervisor de una sola zona que se configura con redes de VDS es compatible con la implementación de clústeres de Tanzu Kubernetes que se crean con Tanzu Kubernetes Grid. No admite la ejecución de pods de vSphere aparte de las implementadas por servicios de supervisor.

Nota Una vez que implemente una instancia de Supervisor en un clúster de vSphere único, lo que provocará la creación de una zona de vSphere, no podrá expandir Supervisor a una implementación de tres zonas. Puede implementar una instancia de Supervisor en una zona de vSphere (implementación de un solo clúster) o en tres zonas de vSphere.

Requisitos previos

- Complete los requisitos previos para configurar clústeres de vSphere como un Supervisor. Consulte Requisitos previos para configurar vSphere IaaS control plane en clústeres de vSphere.

Procedimiento

1. En el menú de inicio, seleccione **Administración de cargas de trabajo**.
2. Seleccione una opción de licencias para Supervisor.
   - Si tiene una licencia de Tanzu Edition válida, haga clic en **Agregar licencia** para agregar la clave de licencia al inventario de licencias de vSphere.

- Si aún no tiene una licencia de Tanzu Edition, introduzca los detalles de contacto para poder recibir la comunicación de VMware y haga clic en **Comenzar**.

El período de evaluación de Supervisor dura 60 días. Dentro de ese período, debe asignar una licencia válida de Tanzu Edition al clúster. Si agregó una clave de licencia de Tanzu Edition, podrá asignar esa misma clave en el período de evaluación de 60 días una vez que haya completado la configuración de Supervisor.

3 En la pantalla **Administración de cargas de trabajo**, haga clic de nuevo en **Comenzar**.

4 Seleccione la página **vCenter Server y red** y el sistema vCenter Server que se configuró para la implementación de Supervisor. A continuación, seleccione **vSphere Distributed Switch (VDS)** como pila de redes y haga clic en **Siguiente**.

5 Para habilitar un Supervisor de zona única, seleccione **IMPLEMENTACIÓN DE CLÚSTER** en la página de ubicación del Supervisor.

Al habilitar la administración de cargas de trabajo en un Supervisor de zona única, se crea automáticamente una zona de vSphere y se asigna el clúster a la zona.

6 Seleccione un clúster de la lista de destinos compatibles.

7 Introduzca un nombre para Supervisor.

8 (opcional) Introduzca un nombre para la zona de vSphere y haga clic en **SIGUIENTE**.

Si no introduce un nombre para la zona de vSphere, se asignará un nombre automáticamente y no podrá cambiarlo más adelante.

9 En la página **Almacenamiento**, configure el almacenamiento para la colocación de máquinas virtuales del plano de control.

Opción	Descripción
Nodo del plano de control	Seleccione la directiva de almacenamiento para la colocación de las máquinas virtuales del plano de control.

10 En la pantalla **Equilibrador de carga**, configure los ajustes de un equilibrador de carga.

a Introduzca un nombre para el equilibrador de carga.

b Seleccione el tipo de equilibrador de carga.

Puede seleccionar entre **NSX Advanced Load Balancer** y **HAProxy**.

c Configurar los ajustes del equilibrador de carga

- Introduzca la siguiente configuración para NSX Advanced Load Balancer:

Opción	Descripción
Nombre	Introduzca un nombre para NSX Advanced Load Balancer.
Endpoint de la controladora de NSX Advanced Load Balancer	Dirección IP del controlador de NSX Advanced Load Balancer. El puerto predeterminado es `443`.
Nombre de usuario	El nombre de usuario que está configurado con NSX Advanced Load Balancer. Utilice este nombre de usuario para acceder al controlador.
Contraseña	La contraseña para el nombre de usuario.
Certificado de servidor	El certificado utilizado por el controlador. Puede proporcionar el certificado que asignó durante la configuración. Para obtener más información, consulte Asignar un certificado al controlador.
Nombre de nube	Introduzca el nombre de la nube personalizada que configuró. Tenga en cuenta que el nombre de la nube distingue entre mayúsculas y minúsculas. Para utilizar **Default-Cloud**, deje este campo vacío. Para obtener más información, consulte Configurar el controlador.

- Introduzca la siguiente configuración para HAProxy:

Opción	Descripción
Endpoint de la controladora de equilibrador de carga de HAProxy	La dirección IP y el puerto de la API del plano de datos de HAProxy, que es la dirección IP de administración del dispositivo de HAProxy. Este componente controla el servidor de HAProxy y se ejecuta dentro de la máquina virtual de HAProxy.
Nombre de usuario	El nombre de usuario que está configurado con el archivo OVA de HAProxy. Este nombre se utiliza para autenticarse con la API del plano de datos de HAProxy.
Contraseña	La contraseña para el nombre de usuario.

<table>
<tr><th>Opción</th><th>Descripción</th></tr>
<tr><td>Rangos de direcciones IP virtuales</td><td>El rango de direcciones IP que utilizan los clústeres de Tanzu Kubernetes en la red de cargas de trabajo. Este rango de IP proviene de la lista de direcciones IP que se definieron en el CIDR que configuró durante la implementación del dispositivo de HAProxy. Puede establecer todo el rango configurado en la implementación de HAProxy, pero también puede establecer un subconjunto de ese CIDR si desea crear varios Supervisores y utilizar direcciones IP de ese rango de CIDR. Este rango no debe superponerse con el rango de IP definido para la red de cargas de trabajo en este asistente. El rango tampoco debe superponerse con ningún ámbito DHCP en esta red de cargas de trabajo.</td></tr>
<tr><td>Certificado TLS de administración de HAProxy</td><td>El certificado en formato PEM que está firmado o es una raíz de confianza del certificado de servidor que presenta la API del plano de datos.

Opción 1: Si se habilita el acceso raíz, ejecute SSH en la máquina virtual de HAProxy como usuario raíz y copie <code>/etc/haproxy/ca.crt</code> en la Entidad de certificación de servidor. No utilice líneas de escape con el formato <code>\n</code>.
Opción 2: Haga clic con el botón derecho en la máquina virtual de HAProxy y seleccione Editar configuración. Copie el certificado de CA desde el campo correspondiente y conviértalo desde Base64 mediante una herramienta de conversión como https://www.base64decode.org/.
Opción 3: Ejecute el siguiente script de PowerCLI. Reemplace las variables <code>$vc</code>, <code>$vc_user</code> y <code>$vc_password</code> con los valores correspondientes.
<pre>
$vc = "10.21.32.43"
$vc_user =
"administrator@vsphere.local"
$vc_password = "PASSWORD"
Connect-VIServer -User $vc_user
-Password $vc_password -Server $vc
$VMname = "haproxy-demo"
$AdvancedSettingName =
"guestinfo.dataplaneapi.cacert"
$Base64cert = get-vm $VMname |Get-
AdvancedSetting -Name
$AdvancedSettingName
while
([string]::IsNullOrEmpty($Base64cert
.Value)) {
     Write-Host "Waiting for CA
Cert Generation... This may take a
under 5-10
minutes as the VM needs to boot and
generate the CA Cert
</pre>
</td></tr>
</table>

Opción	Descripción
	<pre>(if you haven't provided one already)." $Base64cert = get-vm $VMname | Get-AdvancedSetting -Name $AdvancedSettingName Start-sleep -seconds 2 } Write-Host "CA Cert Found... Converting from BASE64" $cert = [Text.Encoding]::Utf8.GetString([Con vert]::FromBase64String($Base64cert. Value)) Write-Host $cert</pre>

11 En la pantalla **Red de administración**, configure los parámetros de la red que se utilizarán para las máquinas virtuales del plano de control de Kubernetes.

a Seleccione un **Modo de red**.

- **Red DHCP**. En este modo, todas las direcciones IP de la red de administración, como las direcciones IP de las máquinas virtuales del plano de control, una dirección IP flotante, los servidores DNS, DNS, los dominios de búsqueda y el servidor NTP, se adquieren automáticamente desde un servidor DHCP. Para obtener direcciones IP flotantes, el servidor DHCP debe estar configurado para admitir identificadores de cliente. En el modo DHCP, todas las máquinas virtuales del plano de control utilizan identificadores de cliente DHCP estables para adquirir direcciones IP. Estos identificadores de cliente se pueden utilizar para configurar la asignación de direcciones IP estáticas para que las direcciones IP de las máquinas virtuales del plano de control en el servidor DHCP se aseguren de que no cambien. No se admite el cambio de las direcciones IP de las máquinas virtuales del plano de control, así como las direcciones IP flotantes.

  Es posible anular algunos de los ajustes heredados de DHCP. Para ello, introduzca valores en los campos de texto de estos ajustes.

Opción	Descripción
Red	Seleccione la red que controlará el tráfico de administración para el Supervisor
IP flotante	Introduzca una dirección IP que determine el punto de inicio para reservar cinco direcciones IP consecutivas para las máquinas virtuales del plano de control de Kubernetes de la siguiente manera: ■ Una dirección IP para cada una de las máquinas virtuales del plano de control de Kubernetes. ■ Una dirección IP flotante para una de las máquinas virtuales del plano de control de Kubernetes a la que se prestará servicio como una interfaz a la red de administración. La máquina virtual del plano de control que tiene asignada la dirección IP flotante actúa como una máquina virtual principal para las tres máquinas virtuales del plano de control de Kubernetes. La dirección IP flotante se traslada al nodo del plano de control que es el líder de etcd en este clúster de Kubernetes. Esto mejora la disponibilidad en el caso de un evento de partición de red. ■ Una dirección IP que se va a utilizar como búfer en caso de que una máquina virtual de plano de control de Kubernetes falle y se ponga en marcha una nueva máquina virtual de plano de control para reemplazarla.

Opción	Descripción
Servidores DNS	Introduzca las direcciones de los servidores DNS que utiliza en su entorno. Si el sistema vCenter Server está registrado con un FQDN, debe introducir las direcciones IP de los servidores DNS que utiliza con el entorno de vSphere para que el FQDN se pueda resolver en el Supervisor.
Dominios de búsqueda DNS	Introduzca los nombres de dominio que DNS busca dentro de los nodos del plano de control de Kubernetes, como `corp.local`, para que el servidor DNS pueda resolverlos.
Servidores NTP	Introduzca las direcciones de los servidores NTP que utiliza en su entorno, si los hubiera.

- **Estático**. Introduzca manualmente toda la configuración de red de la red de administración.

Opción	Descripción
Red	Seleccione la red que controlará el tráfico de administración para el Supervisor
Dirección IP inicial	Introduzca una dirección IP que determine el punto de inicio para reservar cinco direcciones IP consecutivas para las máquinas virtuales del plano de control de Kubernetes de la siguiente manera: ■ Una dirección IP para cada una de las máquinas virtuales del plano de control de Kubernetes. ■ Una dirección IP flotante para una de las máquinas virtuales del plano de control de Kubernetes a la que se prestará servicio como una interfaz a la red de administración. La máquina virtual del plano de control que tiene asignada la dirección IP flotante actúa como una máquina virtual principal para las tres máquinas virtuales del plano de control de Kubernetes. La dirección IP flotante se traslada al nodo del plano de control que es el líder de etcd en este clúster de Kubernetes. Esto mejora la disponibilidad en el caso de un evento de partición de red. ■ Una dirección IP que se va a utilizar como búfer en caso de que una máquina virtual de plano de control de Kubernetes falle y se ponga en marcha una nueva máquina virtual de plano de control para reemplazarla.
Máscara de subred	Solo se aplica a la configuración de IP estática. Introduzca una máscara de subred para la red de administración. Por ejemplo, `255.255.255.0`

Opción	Descripción
Puerta de enlace	Introduzca una puerta de enlace para la red de administración.
Servidores DNS	Introduzca las direcciones de los servidores DNS que utiliza en su entorno. Si el sistema vCenter Server está registrado con un FQDN, debe introducir las direcciones IP de los servidores DNS que utiliza con el entorno de vSphere para que el FQDN se pueda resolver en el Supervisor.
Dominios de búsqueda DNS	Introduzca los nombres de dominio que DNS busca dentro de los nodos del plano de control de Kubernetes, como `corp.local`, para que el servidor DNS pueda resolverlos.
Servidores NTP	Introduzca las direcciones de los servidores NTP que utiliza en su entorno, si los hubiera.

b Haga clic en **Siguiente**.

12 En la página **Red de carga de trabajo**, introduzca la configuración de la red que controlará el tráfico de red de las cargas de trabajo de Kubernetes que se ejecutan en Supervisor.

Nota Si selecciona el uso de un servidor DHCP para proporcionar la configuración de red para las redes de carga de trabajo, no podrá crear ninguna red de carga de trabajo nueva una vez que complete la configuración del Supervisor.

a Seleccione un modo de red.

- **Red DHCP**. En este modo de red, toda la configuración de red de las redes de carga de trabajo se adquiere a través de DHCP. También es posible anular algunos de los ajustes heredados de DHCP. Para ello, introduzca valores en los campos de texto de estos ajustes:

  Nota La configuración de DHCP para redes de cargas de trabajo no es compatible con servicios de supervisor en un Supervisor configurado con la pila de VDS. Para utilizar servicios de supervisor, configure redes de carga de trabajo con direcciones IP estáticas. Puede seguir utilizando DHCP para la red de administración.

Opción	Descripción
Red interna para servicios de Kubernetes	Introduzca una anotación de CIDR que determine el rango de direcciones IP para los clústeres y los servicios de Tanzu Kubernetes que se ejecutan dentro de los clústeres.
Grupo de puertos	Seleccione el grupo de puertos que servirá como red de carga de trabajo principal en el Supervisor. La red principal controla el tráfico de las máquinas virtuales del plano de control de Kubernetes y el tráfico de las cargas de trabajo de Kubernetes. En función de la topología de red, podrá asignar más adelante un grupo de puertos diferente que sirva como red para cada espacio de nombres. De esta forma, podrá proporcionar aislamiento de capa 2 entre los espacios de nombres en Supervisor. Los espacios de nombres que no tienen un grupo de puertos diferente asignado como red usan la red principal. Los clústeres de Tanzu Kubernetes solo usan la red que está asignada al espacio de nombres en el que se implementan o bien utilizan la red principal si no hay ninguna red explícita asignada a ese espacio de nombres.
Nombre de red	Introduzca el nombre de la red.
Servidores DNS	Introduzca las direcciones IP de los servidores DNS que utiliza con su entorno, si los hubiera. Por ejemplo, `10.142.7.1`.

Opción	Descripción
	Cuando se introduce la dirección IP del servidor DNS, se agrega una ruta estática a cada máquina virtual del plano de control. Esto indica que el tráfico a los servidores DNS pasa por la red de cargas de trabajo. Si los servidores DNS que especifica se comparten entre la red de administración y la red de cargas de trabajo, las búsquedas de DNS en las máquinas virtuales del plano de control se enrutan a través de la red de cargas de trabajo después de la configuración inicial.
Servidores NTP	Introduzca la dirección del servidor NTP que utiliza con su entorno si existe alguno.

- **Estático**. Configure manualmente los ajustes de la red de carga de trabajo

Opción	Descripción
Red interna para servicios de Kubernetes	Introduzca una anotación de CIDR que determine el rango de direcciones IP para los clústeres y los servicios de Tanzu Kubernetes que se ejecutan dentro de los clústeres.
Grupo de puertos	Seleccione el grupo de puertos que servirá como red de carga de trabajo principal en el Supervisor. La red principal controla el tráfico de las máquinas virtuales del plano de control de Kubernetes y el tráfico de las cargas de trabajo de Kubernetes. En función de la topología de red, podrá asignar más adelante un grupo de puertos diferente que sirva como red para cada espacio de nombres. De esta forma, podrá proporcionar aislamiento de capa 2 entre los espacios de nombres en Supervisor. Los espacios de nombres que no tienen un grupo de puertos diferente asignado como red usan la red principal. Los clústeres de Tanzu Kubernetes solo usan la red que está asignada al espacio de nombres en el que se implementan o bien utilizan la red principal si no hay ninguna red explícita asignada a ese espacio de nombres.
Nombre de red	Introduzca el nombre de la red.
Rangos de direcciones IP	Introduzca un rango de direcciones IP para asignar la dirección IP de las máquinas virtuales y las cargas de trabajo del plano de control de Kubernetes.

Opción	Descripción
	Este rango de direcciones conecta los nodos del Supervisor y, en el caso de una sola red de cargas de trabajo, también conecta los nodos del clúster de Tanzu Kubernetes. Este rango de direcciones IP no debe superponerse con el rango de VIP del equilibrador de carga cuando se utiliza la configuración **Predeterminado** para HAProxy.
Máscara de subred	Introduzca la dirección IP de la máscara de subred.
Puerta de enlace	Introduzca la puerta de enlace de la red principal.
Servidores NTP	Introduzca la dirección del servidor NTP que utiliza con su entorno si existe alguno.
Servidores DNS	Introduzca las direcciones IP de los servidores DNS que utiliza con su entorno, si los hubiera. Por ejemplo, `10.142.7.1`.

b Haga clic en **Siguiente**.

13 En la página **Revisar y confirmar**, desplácese hacia arriba, revise todos los ajustes que configuró hasta el momento y establezca los ajustes avanzados para la implementación de Supervisor.

Opción	Descripción
Tamaño del plano de control del supervisor	Seleccione el tamaño de las máquinas virtuales del plano de control. El tamaño de las máquinas virtuales del plano de control determina la cantidad de cargas de trabajo que puede ejecutar en Supervisor. Puede elegir lo siguiente: ■ Muy pequeño: 2 CPU, 8 GB de memoria, 32 GB de almacenamiento ■ Pequeño: 4 CPU, 16 GB de memoria, 32 GB de almacenamiento ■ Mediano: 8 CPU, 16 GB de memoria, 32 GB de almacenamiento ■ Grande: 16 CPU, 32 GB de memoria, 32 GB de almacenamiento **Nota** Una vez que seleccione el tamaño del plano de control, solo podrá escalar verticalmente. No podrá escalar horizontalmente a un tamaño menor.
Nombres DNS del servidor de API	De forma opcional, introduzca los FQDN que se utilizarán para acceder al plano de control de Supervisor, en lugar de utilizar la dirección IP del plano de control de Supervisor. Los FQDN que introduzca se integrarán en un certificado generado automáticamente. Al utilizar los FQDN para el Supervisor, puede omitir la especificación de un espacio de IP en el certificado del equilibrador de carga.
Exportar configuración	Exporte un archivo JSON que contenga los valores que introdujo de la configuración de Supervisor. Luego puede modificar e importar el archivo si desea volver a implementar Supervisor o implementar un nuevo Supervisor con una configuración similar. La exportación de la configuración de Supervisor puede ahorrar tiempo porque no se tienen que volver a introducir todos los valores de configuración en este asistente en caso de volver a implementar Supervisor.

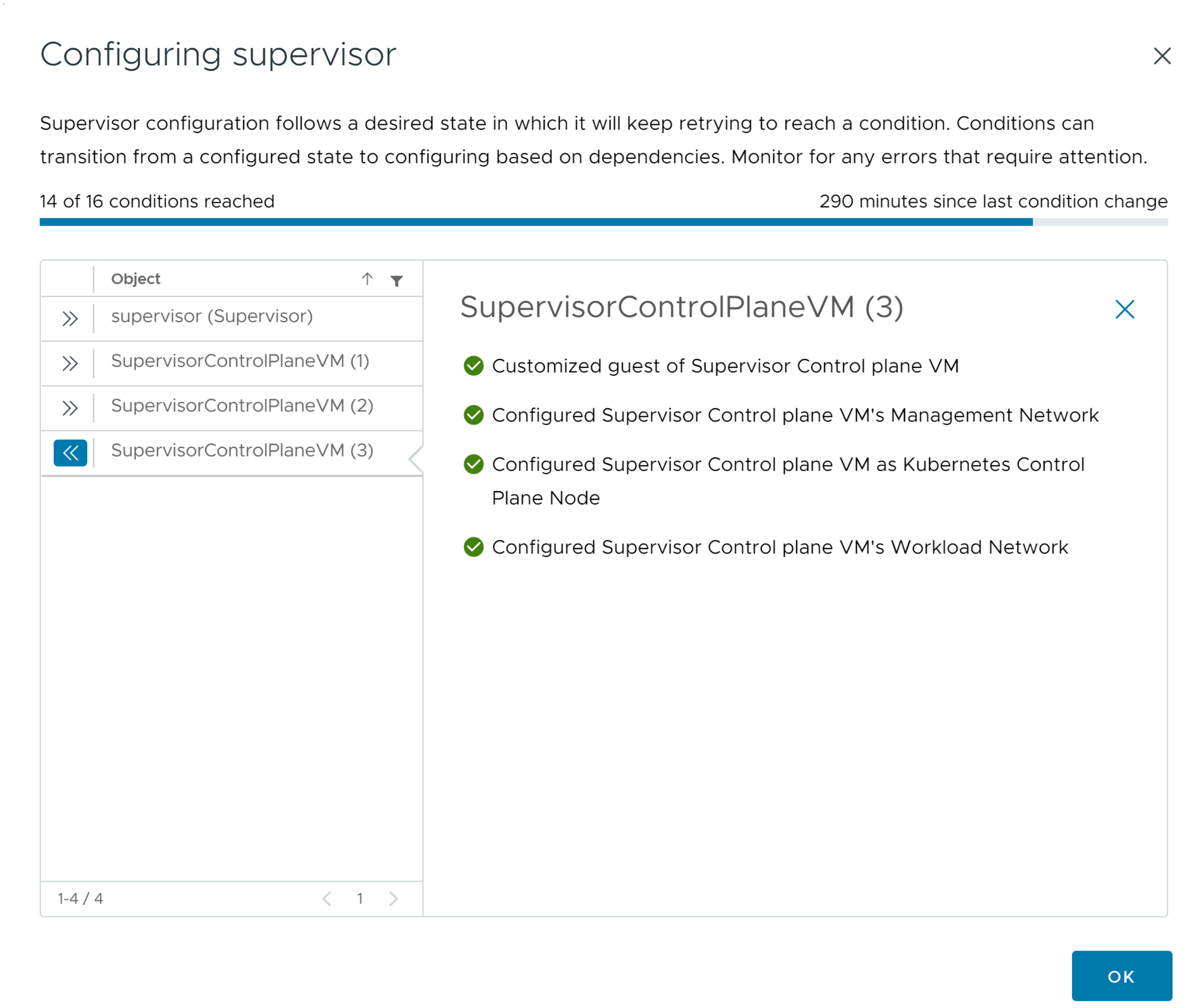
14 Haga clic en **Finalizar** cuando haya terminado de revisar la configuración.

La implementación del Supervisor inicia la creación y la configuración de las máquinas virtuales del plano de control y otros componentes.

Pasos siguientes

Una vez completado el asistente para habilitar Supervisor, podrá realizar un seguimiento del proceso de activación y observar los posibles problemas que se deban solucionar. En la columna **Estado de configuración**, haga clic en **Ver** junto al estado del Supervisor.

Figura 6-1. Vista de activación del supervisor



Para que se complete el proceso de implementación, el Supervisor debe alcanzar el estado deseado, lo que significa que se cumplen todas las condiciones. Cuando un Supervisor se habilita correctamente, su estado cambia de Configurando a En ejecución. Mientras el Supervisor se encuentra en el estado Configurando, se vuelve a intentar de forma continua alcanzar cada una de las condiciones. Si no se alcanza una condición, se vuelve a intentar la operación hasta que se completa correctamente. Por este motivo, el número de condiciones que se alcanzan puede cambiar una y otra vez, por ejemplo, *10 de 16 condiciones alcanzadas*, luego *4 de 16 condiciones alcanzadas* y así sucesivamente. En casos excepcionales, el estado puede cambiar a Error si existen errores que impiden alcanzar el estado deseado.

Para obtener más información sobre los errores de implementación y la forma de solucionarlos, consulte Resolver los estados de errores en las máquinas virtuales del plano de control de un Supervisor durante una activación o una actualización.

Si desea volver a implementar Supervisor modificando los valores de configuración que introdujo en el asistente, revise Capítulo 9 Implementar un Supervisor mediante la importación de un archivo de configuración JSON.

Implementar un Supervisor de zona única con redes de NSX

Obtenga información sobre cómo implementar un Supervisor con redes de NSX en un clúster de vSphere que se asigna a una zona de vSphere. El Supervisor resultante obtendrá alta disponibilidad de nivel de host a través de vSphere HA. Un Supervisor de zona única admite todos los clústeres de Tanzu Kubernetes, las máquinas virtuales y los pods de vSphere.

Si configuró la versión 4.1.1 o posterior de NSX e instaló, configuró y registró la versión 22.1.4 o posterior de NSX Advanced Load Balancer con licencia Enterprise en NSX, el equilibrador de carga que se utilizará con NSX es NSX Advanced Load Balancer. Si configuró versiones de NSX anteriores a la 4.1.1, se utilizará el equilibrador de carga de NSX. Para obtener información, consulte Capítulo 7 Comprobar el equilibrador de carga utilizado con redes NSX.

Nota Una vez que implemente una instancia de Supervisor en un clúster de vSphere único, lo que provocará la creación de una zona de vSphere, no podrá expandir Supervisor a una implementación de tres zonas. Puede implementar una instancia de Supervisor en una zona de vSphere (implementación de un solo clúster) o en tres zonas de vSphere.

Requisitos previos

Compruebe que el entorno cumpla con los requisitos previos para configurar un clúster de vSphere como un Supervisor. Para obtener información sobre los requisitos, consulte Requisitos previos para configurar vSphere IaaS control plane en clústeres de vSphere.

Procedimiento

1 En el menú de inicio, seleccione **Administración de cargas de trabajo**.

2 Seleccione una opción de licencias para Supervisor.

   - Si tiene una licencia de Tanzu Edition válida, haga clic en **Agregar licencia** para agregar la clave de licencia al inventario de licencias de vSphere.
   - Si aún no tiene una licencia de Tanzu Edition, introduzca los detalles de contacto para poder recibir la comunicación de VMware y haga clic en **Comenzar**.

   El período de evaluación de Supervisor dura 60 días. Dentro de ese período, debe asignar una licencia válida de Tanzu Edition al clúster. Si agregó una clave de licencia de Tanzu Edition, podrá asignar esa misma clave en el período de evaluación de 60 días una vez que haya completado la configuración de Supervisor.

3 En la pantalla **Administración de cargas de trabajo**, haga clic de nuevo en **Comenzar**.

4 En la página **vCenter Server y red**, seleccione el sistema vCenter Server que se configuró para la implementación del Supervisor y seleccione **NSX** como pila de redes.

5 En la página **Ubicación de supervisor**, seleccione **Implementación de clúster**.

   a Introduzca un nombre para el nuevo Supervisor.

   b Seleccione un clúster de vSphere compatible.

   c Introduzca un nombre para la zona de vSphere que se creará automáticamente para el clúster que seleccione.

   Si no proporciona un nombre para la zona, se generará uno automáticamente.

   d Haga clic en **Siguiente**.

6 Seleccione directivas de almacenamiento para el Supervisor.

La directiva de almacenamiento que seleccione para cada uno de los siguientes objetos garantiza que el objeto se coloque en el almacén de datos al que se hace referencia en la directiva de almacenamiento. Puede utilizar directivas de almacenamiento iguales o diferentes para los objetos.

Opción	Descripción
Directiva de almacenamiento del plano de control	Seleccione la directiva de almacenamiento para la colocación de las máquinas virtuales del plano de control.
Directiva de almacenamiento de discos efímeros	Seleccione la directiva de almacenamiento para la colocación de los pods de vSphere.
Directiva de almacenamiento de caché de imágenes	Seleccione la directiva de almacenamiento para la colocación de la memoria caché de las imágenes de contenedor.

7 En la pantalla **Red de administración**, configure los parámetros de la red que se utilizarán para las máquinas virtuales del plano de control de Kubernetes.

a Seleccione un **Modo de red**.

- **Red DHCP**. En este modo, todas las direcciones IP de la red de administración, como las direcciones IP de las máquinas virtuales del plano de control, los servidores DNS, DNS, los dominios de búsqueda y el servidor NTP, se adquieren automáticamente desde un servidor DHCP.
- **Estático**. Introduzca manualmente toda la configuración de red de la red de administración.

b Configure los parámetros de la red de administración.

Si seleccionó el modo de red DHCP, pero desea anular la configuración adquirida en el DHCP, haga clic en **Configuración adicional** e introduzca nuevos valores. Si seleccionó el modo de red estática, rellene manualmente los valores de configuración de la red de administración.

Opción	Descripción
Red	Seleccione una red que tenga un adaptador de VMkernel configurado para el tráfico de administración.
Iniciar la dirección IP de control	Introduzca una dirección IP que determine el punto de inicio para reservar cinco direcciones IP consecutivas para las máquinas virtuales del plano de control de Kubernetes de la siguiente manera: ■ Una dirección IP para cada una de las máquinas virtuales del plano de control de Kubernetes. ■ Una dirección IP flotante para una de las máquinas virtuales del plano de control de Kubernetes a la que se prestará servicio como una interfaz a la red de administración. La máquina virtual del plano de control que tiene asignada la dirección IP flotante actúa como una máquina virtual principal para las tres máquinas virtuales del plano de control de Kubernetes. La dirección IP flotante se traslada al nodo del plano de control que es el líder de etcd en este clúster de Kubernetes, que es Supervisor. Esto mejora la disponibilidad en el caso de un evento de partición de red. ■ Una dirección IP que se va a utilizar como búfer en caso de que una máquina virtual de plano de control de Kubernetes falle y se ponga en marcha una nueva máquina virtual de plano de control para reemplazarla.
Máscara de subred	Solo se aplica a la configuración de IP estática. Introduzca una máscara de subred para la red de administración. Por ejemplo, `255.255.255.0`
Servidores DNS	Introduzca las direcciones de los servidores DNS que utiliza en su entorno. Si el sistema vCenter Server está registrado con un FQDN, debe introducir las direcciones IP de los servidores DNS que utiliza con el entorno de vSphere para que el FQDN se pueda resolver en el Supervisor.

Opción	Descripción
Dominios de búsqueda DNS	Introduzca los nombres de dominio que DNS busca dentro de los nodos del plano de control de Kubernetes, como `corp.local`, para que el servidor DNS pueda resolverlos.
NTP	Introduzca las direcciones de los servidores NTP que utiliza en su entorno, si los hubiera.

8 En el panel **Red de cargas de trabajo**, configure las opciones de las redes para los espacios de nombres.

Opción	Descripción
vSphere Distributed Switch	Seleccione la instancia de vSphere Distributed Switch que controla las redes de superposición para Supervisor. Por ejemplo, seleccione `DSwitch`.
servidor DNS	Introduzca las direcciones IP de los servidores DNS que utiliza con su entorno, si los hubiera. Por ejemplo, `10.142.7.1`.
Modo NAT	El modo NAT está seleccionado de forma predeterminada. Si anula la selección de la opción, se podrá acceder directamente a todas las cargas de trabajo, como los pods de vSphere, las máquinas virtuales y las direcciones IP de los nodos de los clústeres de Tanzu Kubernetes desde fuera de la puerta de enlace de nivel 0, y no tendrá que configurar los CIDR de salida. **Nota** Si anula la selección del modo NAT, no se admitirá el almacenamiento de volumen de archivos.
Red de espacio de nombres	Introduzca uno o varios CIDR de IP para crear subredes o segmentos y asignar direcciones IP a las cargas de trabajo.
CIDR de entrada	Introduzca una anotación CIDR que determine el rango de IP de entrada para los servicios de Kubernetes. Este rango se utiliza para los servicios de tipo equilibrador de carga y entrada.
Clúster de Edge	Seleccione el clúster de NSX Edge que tenga la puerta de enlace de nivel 0 que desee utilizar para las redes de espacio de nombres. Por ejemplo, seleccione `EDGE-CLUSTER`.
Puerta de enlace de nivel 0	Seleccione la puerta de enlace de nivel 0 que se asociará con la puerta de enlace de nivel 1 del clúster.
Prefijo de subred	Introduzca el prefijo de subred que especifica el tamaño de la subred reservada para los segmentos de espacios de nombres. El valor predeterminado es 28.
CIDR de servicio	Introduzca una anotación CIDR para determinar el rango de IP de los servicios de Kubernetes. Puede utilizar el valor predeterminado.
CIDR de egreso	Introduzca una anotación CIDR que determine la IP de salida de los servicios de Kubernetes. Solo se asigna una dirección IP de egreso para cada espacio de nombres en el Supervisor. La IP de salida es la dirección IP que las cargas de trabajo de Kubernetes en el espacio de nombres concreto utilizan para comunicarse fuera de NSX.

9 En la página **Revisar y confirmar**, desplácese hacia arriba, revise todos los ajustes que configuró hasta el momento y establezca los ajustes avanzados para la implementación de Supervisor.

Opción	Descripción
Tamaño del plano de control del supervisor	Seleccione el tamaño de las máquinas virtuales del plano de control. El tamaño de las máquinas virtuales del plano de control determina la cantidad de cargas de trabajo que puede ejecutar en Supervisor. Puede elegir lo siguiente: ■ Muy pequeño: 2 CPU, 8 GB de memoria, 32 GB de almacenamiento ■ Pequeño: 4 CPU, 16 GB de memoria, 32 GB de almacenamiento ■ Mediano: 8 CPU, 16 GB de memoria, 32 GB de almacenamiento ■ Grande: 16 CPU, 32 GB de memoria, 32 GB de almacenamiento **Nota** Una vez que seleccione el tamaño del plano de control, solo podrá escalar verticalmente. No podrá escalar horizontalmente a un tamaño menor.
Nombres DNS del servidor de API	De forma opcional, introduzca los FQDN que se utilizarán para acceder al plano de control de Supervisor, en lugar de utilizar la dirección IP del plano de control de Supervisor. Los FQDN que introduzca se integrarán en un certificado generado automáticamente. Al utilizar los FQDN para el Supervisor, puede omitir la especificación de un espacio de IP en el certificado del equilibrador de carga.
Exportar configuración	Exporte un archivo JSON que contenga los valores que introdujo de la configuración de Supervisor. Luego puede modificar e importar el archivo si desea volver a implementar Supervisor o implementar un nuevo Supervisor con una configuración similar. La exportación de la configuración de Supervisor puede ahorrar tiempo porque no se tienen que volver a introducir todos los valores de configuración en este asistente en caso de volver a implementar Supervisor.

10 Haga clic en **Finalizar** cuando haya terminado de revisar la configuración.

La implementación del Supervisor inicia la creación y la configuración de las máquinas virtuales del plano de control y otros componentes.

11 En la pestaña **Supervisores**, realice un seguimiento del proceso de implementación del Supervisor.

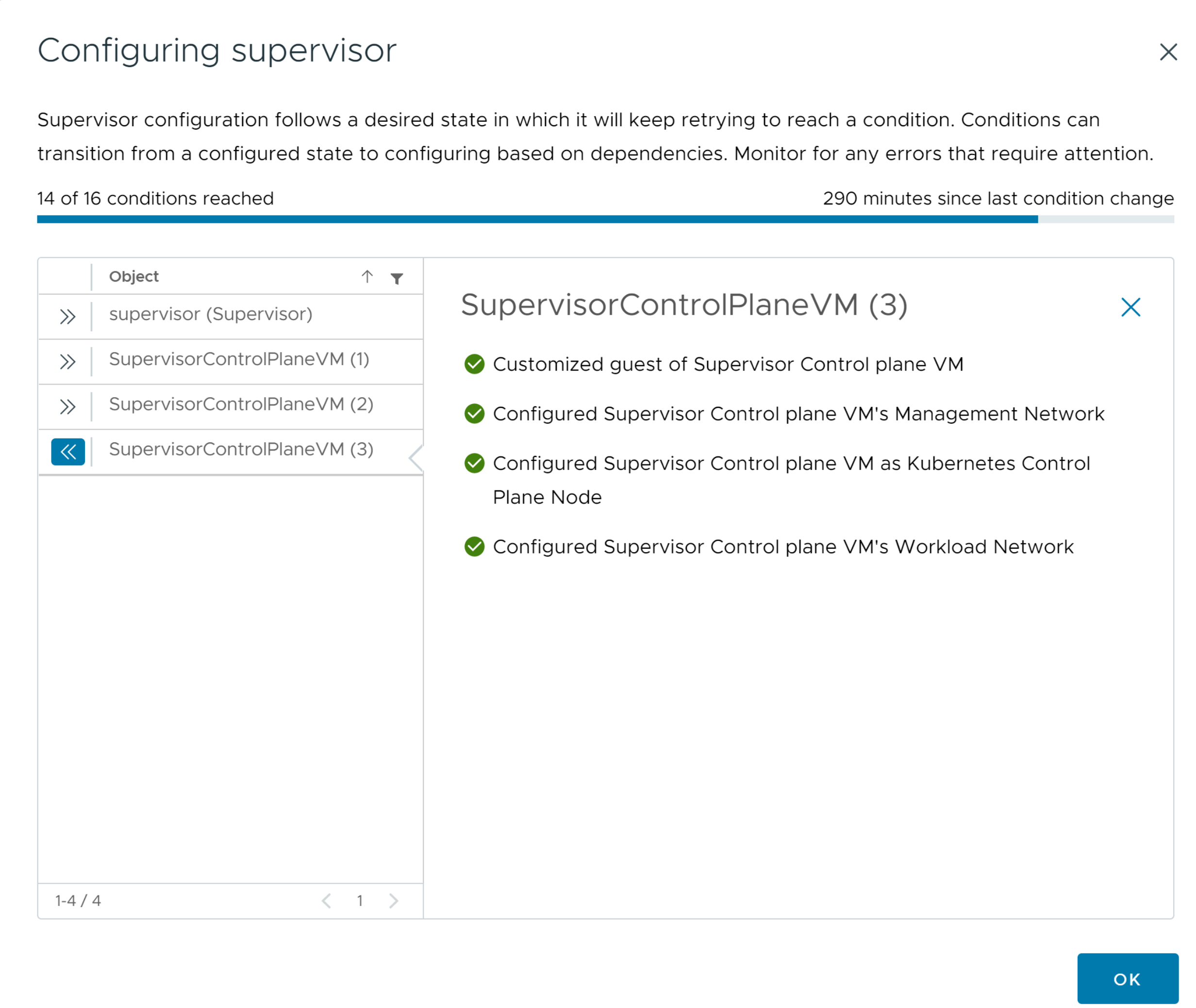
a En la columna **Estado de configuración**, haga clic en **Ver** junto al estado del Supervisor.

b Vea el estado de configuración de cada objeto y realice un seguimiento de los posibles problemas que se deban solucionar.

Pasos siguientes

Una vez completado el asistente para habilitar Supervisor, podrá realizar un seguimiento del proceso de activación y observar los posibles problemas que se deban solucionar. En la columna **Estado de configuración**, haga clic en **Ver** junto al estado del Supervisor.

Figura 6-2. Vista de activación del supervisor



Para que se complete el proceso de implementación, el Supervisor debe alcanzar el estado deseado, lo que significa que se cumplen todas las condiciones. Cuando un Supervisor se habilita correctamente, su estado cambia de Configurando a En ejecución. Mientras el Supervisor se encuentra en el estado Configurando, se vuelve a intentar de forma continua alcanzar cada una de las condiciones. Si no se alcanza una condición, se vuelve a intentar la operación hasta que se completa correctamente. Por este motivo, el número de condiciones que se alcanzan puede cambiar una y otra vez, por ejemplo, *10 de 16 condiciones alcanzadas*, luego *4 de 16 condiciones alcanzadas* y así sucesivamente. En casos excepcionales, el estado puede cambiar a Error si existen errores que impiden alcanzar el estado deseado.

Para obtener más información sobre los errores de implementación y la forma de solucionarlos, consulte Resolver los estados de errores en las máquinas virtuales del plano de control de un Supervisor durante una activación o una actualización.

Si desea volver a implementar Supervisor modificando los valores de configuración que introdujo en el asistente, revise Capítulo 9 Implementar un Supervisor mediante la importación de un archivo de configuración JSON.

Comprobar el equilibrador de carga utilizado con redes NSX

7

Un Supervisor configurado con redes NSX puede utilizar el equilibrador de carga NSX o NSX Advanced Load Balancer.

Si configuró la versión 4.1.1 o posterior de NSX e instaló, configuró y registró NSX Advanced Load Balancer versión 22.1.4 o posterior con la licencia Enterprise en NSX, el equilibrador de carga que se utilizará con NSX es NSX Advanced Load Balancer. Si configuró versiones de NSX anteriores a la 4.1.1, se utilizará el equilibrador de carga de NSX.

Para comprobar qué equilibrador de carga está configurado con NSX, ejecute el siguiente comando:

```
kubectl get gateways.networking.x-k8s.io <gateway> -n <gateway_namespace> -oyaml
```

Si un finalizador de puerta de enlace `gateway.ako.vmware.com` o finalizador de entrada `ingress.ako.vmware.com/finalizer` está en la especificación, indica que NSX Advanced Load Balancer está configurado.

Exportar la configuración de un Supervisor

8

Consulte cómo exportar la configuración de un Supervisor existente, el cual podrá importar posteriormente en el asistente de activación de Supervisor para implementar una nueva instancia de Supervisor con una configuración similar. El Supervisor se exporta en un archivo de configuración JSON, que puede modificar según sea necesario y puede utilizar para implementar una instancia de Supervisor nueva.

La exportación de una configuración de Supervisor le permite hacer lo siguiente:

- Persistencia de configuraciones de Supervisor. Puede exportar todas las configuraciones de Supervisor anteriores y reutilizarlas cuando sea necesario.
- Solución de problemas más eficiente. Si se produce un error en la activación de un Supervisor, puede ajustar la configuración de Supervisor directamente en el archivo JSON y reiniciar el proceso. Esto permite solucionar problemas rápidamente, ya que puede modificar la configuración directamente en el archivo JSON antes de importarlo.
- Administración optimizada. Puede compartir la configuración de Supervisor exportada con otros administradores para configurar nuevos Supervisores con opciones similares.
- Formato coherente. Las configuraciones de Supervisor exportadas siguen un formato estandarizado que se aplica a los tipos de implementación compatibles.

También puede exportar la configuración de Supervisor durante el flujo de trabajo de activación de Supervisor. Para obtener más información, consulte Capítulo 5 Implementar Supervisor de tres zonas y Capítulo 6 Implementar un Supervisor de una sola zona .

Requisitos previos

Implemente un Supervisor.

Procedimiento

1 Vaya a **Administración de cargas de trabajo > Supervisor > Supervisores**.

2 Seleccione un Supervisor y seleccione **Exportar configuración**.

Resultados

La configuración se exporta y se guarda en un archivo ZIP denominado `wcp-config.zip` que se almacena en local en la carpeta de descargas predeterminada del navegador. Dentro del archivo `wcp-config.zip` puede encontrar lo siguiente:

- Un archivo JSON que contiene la configuración de Supervisor denominada `wcp-config.jso`. Cada opción de configuración tiene un nombre y una ubicación correspondientes en el archivo JSON. Este archivo JSON se ajusta a una estructura de datos jerárquica.
- Un archivo de esquema JSON válido denominado `wcp-config-schema.json`. Este archivo describe todos los ajustes exportables para el Supervisor, entre los que se incluyen su tipo, la ubicación dentro del archivo JSON y si son obligatorios. Puede utilizar el archivo de esquema para generar un archivo JSON de configuración de ejemplo, el cual puede rellenar manualmente e importar a un flujo de trabajo de activación nuevo.

Pasos siguientes

'

Edite la configuración JSON según sea necesario y utilícela para implementar nuevos Supervisores. Consulte Capítulo 9 Implementar un Supervisor mediante la importación de un archivo de configuración JSON.

Implementar un Supervisor mediante la importación de un archivo de configuración JSON

9

Consulte cómo rellenar automáticamente todos los valores de configuración en el asistente de activación de Supervisor. Para ello, importe un archivo de configuración JSON que haya exportado desde implementaciones de Supervisor anteriores. Al solucionar problemas surgidos en una implementación de Supervisor que no se realizó correctamente o al implementar un Supervisor nuevo con una configuración similar, puede cambiar los valores de configuración directamente en el archivo JSON antes de importarlo en el asistente. De esta manera, se ahorra tiempo al no tener que completar manualmente todos los valores en el asistente y puede concentrarse solo en las áreas que necesitan solución de problemas.

Puede exportar la configuración de un Supervisor de dos formas distintas:

- Durante la implementación de Supervisor en la página **Listo para completar** del asistente. Para obtener más información, consulte Capítulo 5 Implementar Supervisor de tres zonas y Capítulo 6 Implementar un Supervisor de una sola zona .
- Exporte la configuración de un Supervisor ya implementado. Consulte Capítulo 8 Exportar la configuración de un Supervisor.

Requisitos previos

- Complete los requisitos previos para configurar clústeres de vSphere como un Supervisor. Consulte Requisitos previos para configurar vSphere IaaS control plane en clústeres de vSphere.
- Compruebe que tiene un archivo de configuración JSON que haya exportado de una implementación de Supervisor existente. El nombre predeterminado del archivo es `wcp-config.json`.

Procedimiento

1 Comience la implementación de Supervisor de una de las siguientes maneras:

   - Si aún no implementó correctamente Supervisor, haga clic en **Comenzar** en la página **Administración de cargas de trabajo**.
   - Si desea implementar un Supervisor adicional en su entorno, seleccione **Administración de cargas de trabajo > Supervisor > Supervisores > Agregar supervisor**.

2 En la esquina superior derecha, seleccione **Importar configuración**.

   vSphere Client comprueba los valores en el archivo JSON. Es posible que aparezcan errores si el archivo cargado no es válido o el archivo JSON está dañado. Del mismo modo, aparecerán errores si el archivo JSON no tiene la versión de especificación o si la versión de especificación supera la versión que admite actualmente el cliente. Por lo tanto, solo debe editar la configuración que necesita antes de importar el archivo de configuración. Si el archivo está dañado, puede utilizar el esquema JSON para generar una configuración de Supervisor vacía que podrá rellenar con los valores que necesite.

3 En el cuadro de diálogo **Cargar configuración de supervisor**, haga clic en **Cargar** y seleccione un archivo de configuración JSON que haya exportado previamente.

4 Haga clic en **Importar**.

   Los valores registrados en el archivo de configuración JSON se rellenan en el asistente de activación de Supervisor. Es posible que aún tenga que introducir manualmente algunas opciones de ajustes, como la contraseña del equilibrador de carga.

5 Haga clic en **Siguiente** a través del asistente y rellene los valores que sean necesarios.

6 En la página **Revisar y confirmar**, desplácese hacia arriba, revise todos los ajustes que configuró hasta el momento y realice los cambios finales en caso de ser necesario.

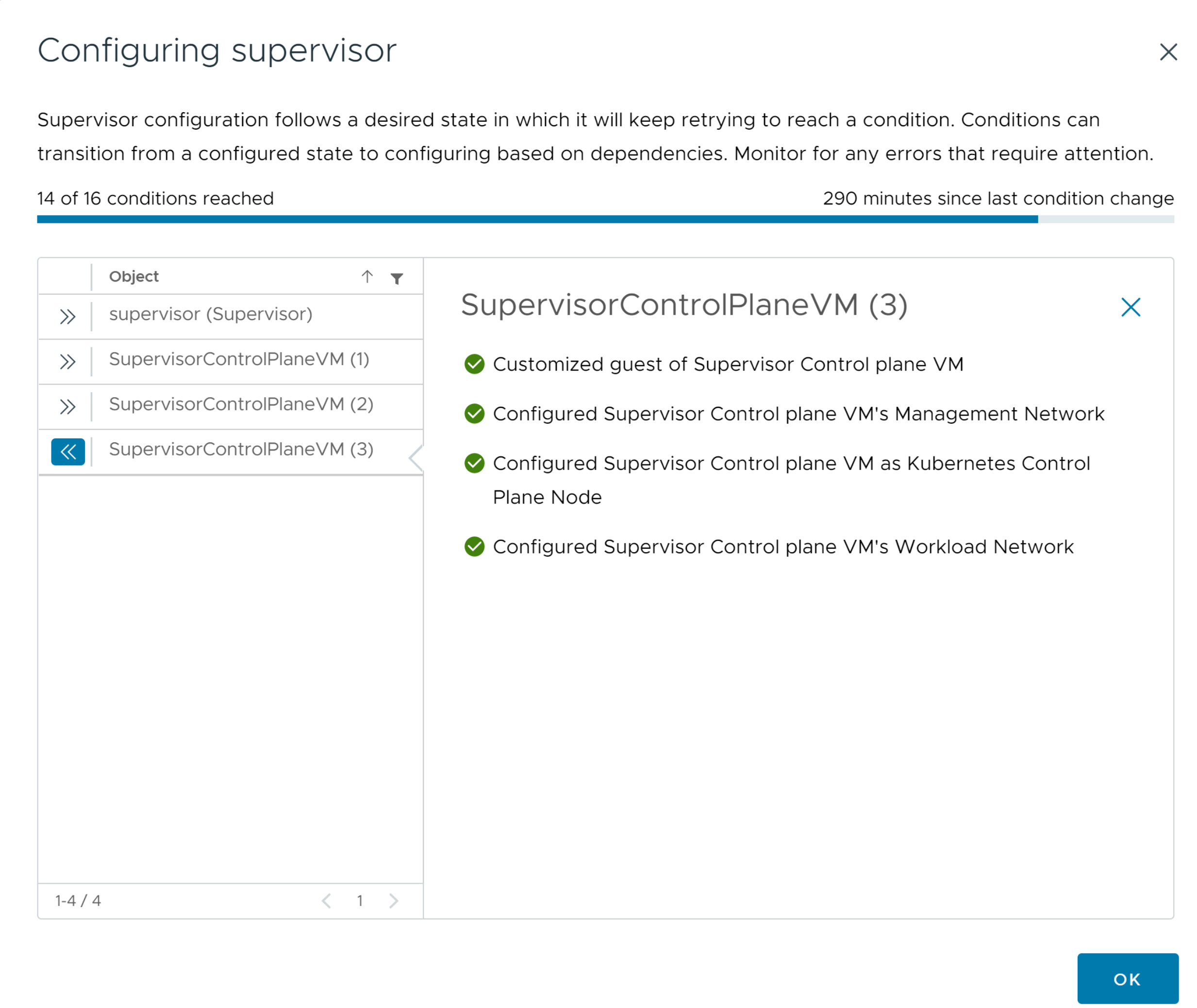
7 Haga clic en **Finalizar** cuando haya terminado de revisar la configuración.

   La activación de Supervisor inicia la creación y la configuración de las máquinas virtuales del plano de control y otros componentes.

Pasos siguientes

Una vez completado el asistente para habilitar Supervisor, podrá realizar un seguimiento del proceso de activación y observar los posibles problemas que se deban solucionar. En la columna **Estado de configuración**, haga clic en **Ver** junto al estado del Supervisor.

Figura 9-1. Vista de activación del supervisor



Para que se complete el proceso de implementación, el Supervisor debe alcanzar el estado deseado, lo que significa que se cumplen todas las condiciones. Cuando un Supervisor se habilita correctamente, su estado cambia de Configurando a En ejecución. Mientras el Supervisor se encuentra en el estado Configurando, se vuelve a intentar de forma continua alcanzar cada una de las condiciones. Si no se alcanza una condición, se vuelve a intentar la operación hasta que se completa correctamente. Por este motivo, el número de condiciones que se alcanzan puede cambiar una y otra vez, por ejemplo, *10 de 16 condiciones alcanzadas*, luego *4 de 16 condiciones alcanzadas* y así sucesivamente. En casos excepcionales, el estado puede cambiar a Error si existen errores que impiden alcanzar el estado deseado.

Para obtener más información sobre los errores de implementación y la forma de solucionarlos, consulte Resolver los estados de errores en las máquinas virtuales del plano de control de un Supervisor durante una activación o una actualización.

Asignar una licencia a Supervisor 10

Si utiliza Supervisor en modo de evaluación, debe asignar al clúster una licencia de solución (VVF o VCF) o una licencia de Tanzu Edition antes de que finalice el período de evaluación de 60 días.

Consulte Licencias para vSphere IaaS control plane si desea obtener información sobre cómo funciona la licencia de Tanzu.

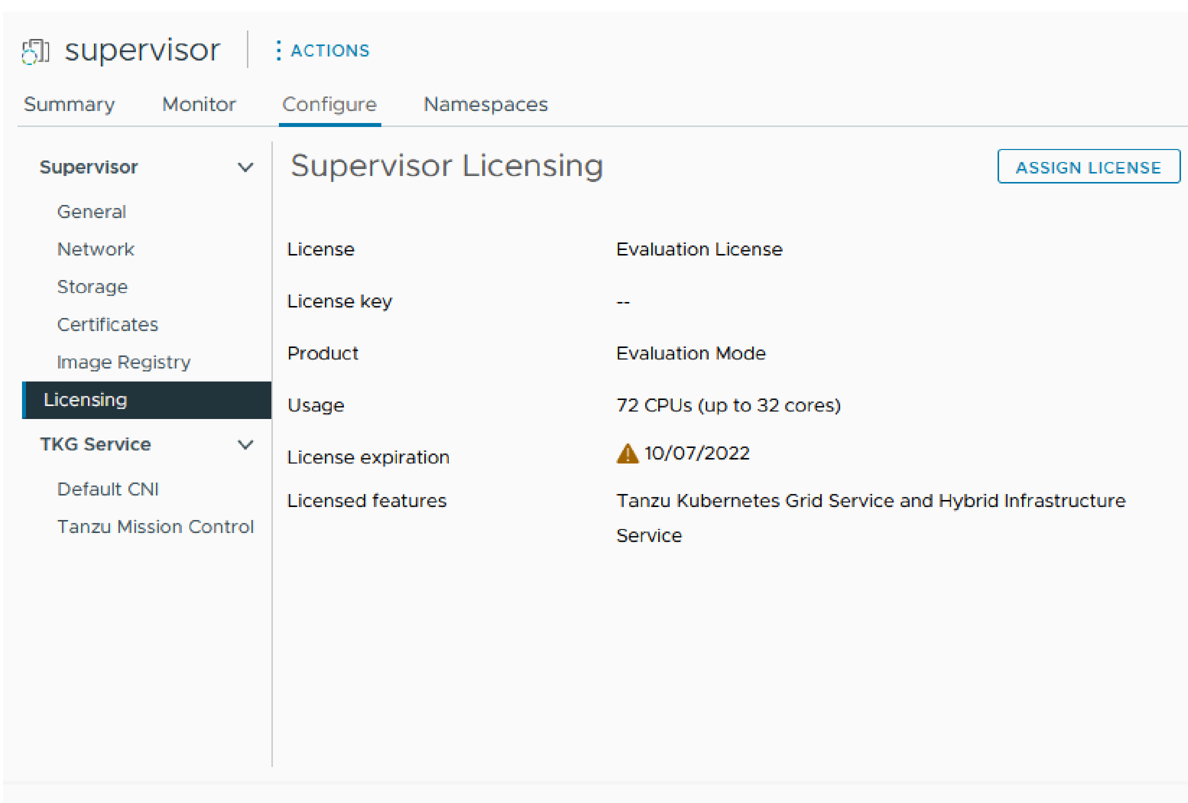
Procedimiento

1 En vSphere Client, desplácese hasta **Administración de cargas de trabajo**.

2 Seleccione **Supervisores** y seleccione el Supervisor en la lista.

3 Seleccione **Configurar > Licencias**.

Figura 10-1. Asignar una licencia a la interfaz de usuario de Supervisor



4 Haga clic en **Asignar licencia**.

5 En el cuadro de diálogo **Asignar licencia**, haga clic en **Nueva licencia**.

6 Introduzca una clave de licencia válida y haga clic en **Aceptar**.

Conectarse a clústeres de vSphere IaaS control plane

11

Conéctese al Supervisor para aprovisionar clústeres de Tanzu Kubernetes, pods de vSphere y máquinas virtuales. Una vez aprovisionados, podrá conectarse a los clústeres de Tanzu Kubernetes Grid mediante diversos métodos y autenticarse según su función y su objetivo.

Lea los siguientes temas a continuación:

- Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere
- Configurar el inicio de sesión seguro para clústeres de vSphere IaaS control plane
- Conectarse al Supervisor como usuario vCenter Single Sign-On
- Conceder acceso de desarrollador a clústeres de Tanzu Kubernetes

Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere

Puede utilizar Herramientas de la CLI de Kubernetes para vSphere para iniciar sesión en el plano de control de Supervisor, acceder a los espacios de nombres de vSphere para los que tiene permisos, e implementar y administrar pods de vSphere, clústeres de Tanzu Kubernetes Grid y máquinas virtuales.

El paquete de descarga de Herramientas de la CLI de Kubernetes incluye dos ejecutables: el kubectl de código abierto estándar y el complemento de vSphere para kubectl. La CLI de kubectl tiene una arquitectura acoplable. El complemento de vSphere para kubectl extiende los comandos disponibles a kubectl de modo que se conecte al Supervisor y a clústeres de Tanzu Kubernetes Grid mediante credenciales de vCenter Single Sign-On.

Nota Como práctica recomendada, una vez que haya realizado una actualización del espacio de nombres de vSphere y haya actualizado el Supervisor, actualice también el complemento de vSphere para kubectl. Consulte Actualizar el complemento de vSphere para kubectl en *Mantenimiento del plano de control de IaaS de vSphere*.

Procedimiento

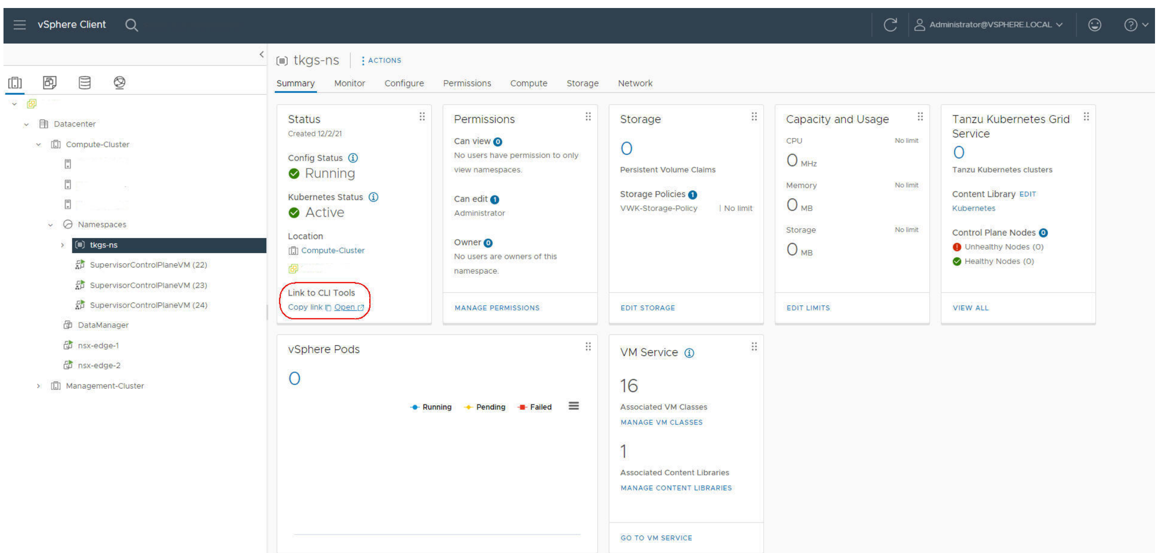
1 Obtenga la dirección IP o el FQDN del plano de control de Supervisor, que es también la URL de descarga de las Herramientas de la CLI de Kubernetes para vSphere.

Si es ingeniero de desarrollo y operaciones y no tiene acceso al entorno de vSphere, puede pedir al administrador de vSphere que realice los siguientes pasos.

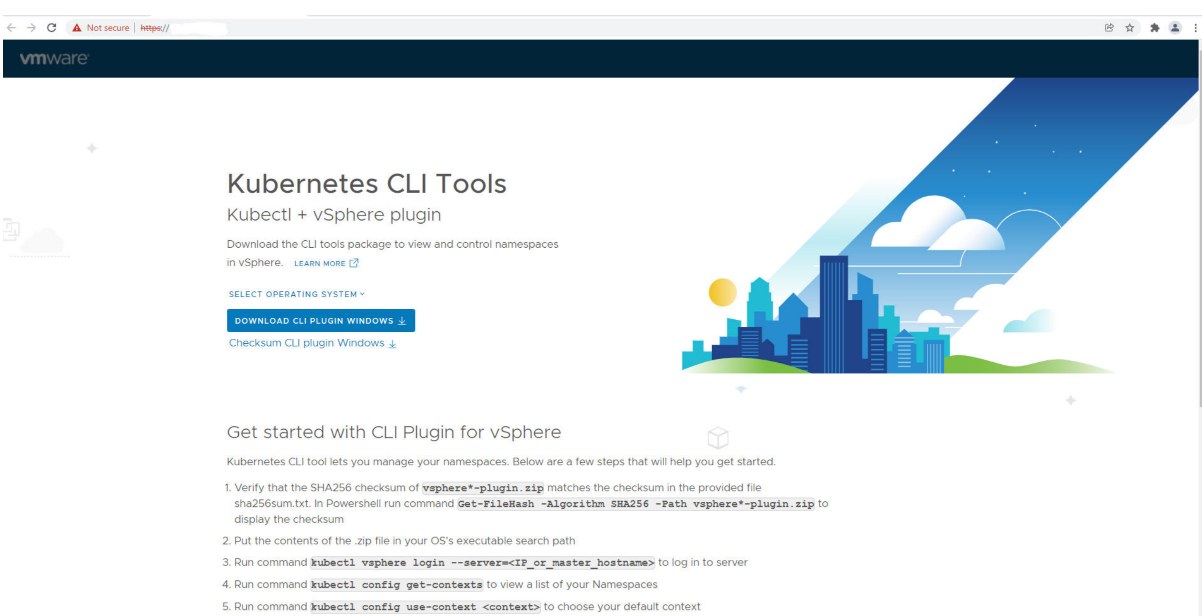
a En vSphere Client, desplácese hasta **Administración de cargas de trabajo > Espacios de nombres** y seleccione un espacio de nombres de vSphere.

b Seleccione la pestaña **Resumen** y localice el panel **Estado**.

c En **Vínculo a herramientas de CLI**, haga clic en **Abrir** o en **Copiar vínculo**.



2 En un navegador, abra la URL de descarga de las **Herramientas de la CLI de Kubernetes**.



3 Seleccione el sistema operativo.

4 Descargue el archivo `vsphere-plugin.zip`.

5 Extraiga el contenido del archivo ZIP en un directorio de trabajo.

   El paquete `vsphere-plugin.zip` contiene dos archivos ejecutables: kubectl y complemento de vSphere para kubectl. `kubectl` es la CLI de Kubernetes estándar. `kubectl-vsphere` es el complemento de vSphere para kubectl que lo ayudará a autenticarse en el Supervisor y en los clústeres de Tanzu Kubernetes utilizando sus credenciales de vCenter Single Sign-On.

6 Agregue la ubicación de los dos archivos ejecutables a la variable PATH del sistema.

7 Para comprobar la instalación de la CLI de kubectl, inicie una sesión de Shell, de terminal o de línea de comandos y ejecute el comando `kubectl`.

   Verá el mensaje de aviso de kubectl y la lista de opciones de línea de comandos para la CLI.

8 Para comprobar la instalación de complemento de vSphere para kubectl, ejecute el comando `kubectl vsphere`.

   Verá el mensaje de aviso de complemento de vSphere para kubectl y la lista de opciones de línea de comandos para el complemento.

Pasos siguientes

Configurar el inicio de sesión seguro para clústeres de vSphere IaaS control plane.

Configurar el inicio de sesión seguro para clústeres de vSphere IaaS control plane

Para iniciar sesión de forma segura en el Supervisor y en clústeres de Tanzu Kubernetes Grid, configure el complemento de vSphere para kubectl con el certificado TLS adecuado y asegúrese de ejecutar la edición más reciente del complemento.

Certificado de CA de Supervisor

vSphere IaaS control plane admite vCenter Single Sign-On para el acceso a los clústeres mediante el comando `kubectl vsphere login …` de complemento de vSphere para kubectl. Para instalar y utilizar esta utilidad, consulte Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere.

El complemento complemento de vSphere para kubectl establece de forma predeterminada el inicio de sesión seguro y requiere un certificado de confianza, el certificado firmado por la entidad de certificación raíz vCenter Server. A pesar de que el complemento admite la marca de `--insecure-skip-tls-verify`, no se recomienda por motivos de seguridad.

Para iniciar sesión de forma segura en los clústeres de Supervisor y Tanzu Kubernetes Grid mediante el complemento complemento de vSphere para kubectl, tiene dos opciones:

Opción	Instrucciones
Descargue e instale el certificado de la entidad de certificación de vCenter Server raíz en cada máquina cliente.	Consulte el artículo VMware de la base de conocimientos Cómo descargar e instalar certificados raíz de vCenter Server.
Reemplace el certificado VIP utilizado para Supervisor por un certificado firmado por una entidad de certificación de confianza de cada máquina cliente.	Consulte Reemplazar el certificado VIP para conectarse de forma segura al endpoint de API de Supervisor.

Nota Para obtener información adicional sobre la autenticación de vSphere, incluidos vCenter Single Sign-On, la administración y rotación de certificados de vCenter Server y la solución de problemas de autenticación, consulte la documentación de autenticación de vSphere. Para obtener más información sobre los certificados de vSphere IaaS control plane, consulte el artículo 89324 de la base de conocimientos de VMware.

Certificado de CA del clúster de Tanzu Kubernetes Grid

Para conectarse de forma segura con el servidor de API del clúster de Tanzu Kubernetes mediante la CLI de `kubectl`, debe descargar el certificado de CA del clúster de Tanzu Kubernetes.

Si utiliza la edición más reciente de complemento de vSphere para kubectl, la primera vez que inicie sesión en el clúster de Tanzu Kubernetes Grid, el complemento registra el certificado de CA del clúster de Tanzu Kubernetes en el archivo `kubconfig`. Este certificado se almacena en el secreto de Kubernetes denominado *`TANZU-KUBERNETES-CLUSTER-NAME`*`-ca`. El complemento utiliza este certificado para rellenar la información de CA en el almacén de datos de CA del clúster correspondiente.

Si va a actualizar vSphere IaaS control plane, asegúrese de hacerlo a la versión más reciente del complemento. Consulte Actualizar el complemento de vSphere para kubectl en *Mantenimiento del plano de control de IaaS de vSphere*.

Conectarse al Supervisor como usuario vCenter Single Sign-On

Para aprovisionar los pods de vSphere, los clústeres de Tanzu Kubernetes Grid o las máquinas virtuales, conéctese al Supervisor mediante el complemento de vSphere para kubectl y autentíquese con las credenciales de vCenter Single Sign-On.

Después de iniciar sesión en el Supervisor, el complemento de vSphere para kubectl genera el contexto del Supervisor. En Kubernetes, un contexto de configuración incluye un Supervisor, un espacio de nombres de vSphere y un usuario. Puede ver el contexto del clúster en el archivo `.kube/config`. Generalmente, este archivo se denomina `kubeconfig`.

Nota Si ya tiene un archivo `kubeconfig`, este se anexa a cada contexto de Supervisor. El complemento de vSphere para kubectl respeta la variable de entorno KUBECONFIG que kubectl utiliza. Aunque no es obligatorio, puede que resulte útil definir esta variable antes de ejecutar `kubectl vsphere login ...` para que la información se escriba en un archivo nuevo (en lugar de agregarse al archivo `kubeconfig` actual).

Requisitos previos

- Obtenga las credenciales de vCenter Single Sign-On del administrador de vSphere.
- Obtenga la dirección IP del plano de control del Supervisor del administrador de vSphere. La dirección IP del plano de control del Supervisor está vinculada en la interfaz de usuario de cada espacio de nombres de vSphere, en **Administración de cargas de trabajo** en vSphere Client.
- Para iniciar sesión mediante un FQDN en lugar de la dirección IP del plano de control, obtenga un FQDN configurado para el Supervisor durante la habilitación.
- Obtenga el nombre del espacio de nombres de vSphere para el que tiene permisos.
- Obtenga la confirmación de que tiene permisos **Editar** en espacio de nombres de vSphere.
- Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere.
- Para comprobar que el certificado ofrecido por el plano de control de Kubernetes sea de confianza en el sistema, instale la CA de firma como raíz de confianza o agregue el certificado directamente como raíz de confianza. Consulte Configurar el inicio de sesión seguro para clústeres de vSphere IaaS control plane.

Procedimiento

1 Para ver la sintaxis y las opciones de los comandos para iniciar sesión, ejecute el siguiente comando.

```
kubectl vsphere login --help
```

2 Para conectarse a Supervisor, ejecute el siguiente comando.

```
kubectl vsphere login --server=<KUBERNETES-CONTROL-PLANE-IP-ADDRESS> --vsphere-username
<VCENTER-SSO-USER>
```

También puede iniciar sesión mediante un FQDN:

```
kubectl vsphere login --server <KUBERNETES-CONTROL-PLANE-FQDN --vsphere-username <VCENTER-
SSO-USER>
```

Por ejemplo:

```
kubectl vsphere login --server=10.92.42.13 --vsphere-username administrator@example.com
```

```
kubectl vsphere login --server wonderland.acme.com --vsphere-username
administrator@example.com
```

Esta acción crea un archivo de configuración con el token web de JSON (JSON Web Token, JWT) para autenticarse en la API de Kubernetes.

3 Para autenticarse, introduzca la contraseña del usuario.

Después de conectarse a Supervisor, se le mostrarán los contextos de configuración a los que puede acceder. Por ejemplo:

```

You have access to the following contexts:
tanzu-ns-1
tkg-cluster-1
tkg-cluster-2
```

4 Para ver los detalles de los contextos de configuración a los que puede acceder, ejecute el siguiente comando de `kubectl`:

```
kubectl config get-contexts
```

La CLI muestra los detalles de cada contexto disponible.

5 Para cambiar de contexto, utilice el siguiente comando:

```
kubectl config use-context <example-context-name>
```

Pasos siguientes

Conéctese a un clúster de Tanzu Kubernetes Grid como vCenter Single Sign-On. Para obtener más información, consulte Conectarse a un clúster de TKG como usuario de vCenter Single Sign-On en *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

Conceder acceso de desarrollador a clústeres de Tanzu Kubernetes

Los desarrolladores son los usuarios de destino de Kubernetes. Una vez que se aprovisione un clúster de Tanzu Kubernetes, puede conceder acceso de desarrollador mediante autenticación de vCenter Single Sign-On.

Autenticación para desarrolladores

Un administrador de clústeres puede otorgar acceso al clúster a otros usuarios, como desarrolladores. Los desarrolladores pueden implementar pods en clústeres directamente mediante sus cuentas de usuario o de forma indirecta a través de cuentas de servicio. Para obtener más información, consulte Otorgar acceso de SSO a clústeres de carga de trabajo a los desarrolladores en *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

- Para la autenticación de la cuenta de usuario, los clústeres de Tanzu Kubernetes admiten usuarios y grupos de vCenter Single Sign-On. El usuario o el grupo pueden ser locales para la instancia de vCenter Server o sincronizarse desde un servidor de directorio compatible.
- Para la autenticación de la cuenta de servicio, puede utilizar tokens de servicio. Para obtener más información, consulte la documentación de Kubernetes.

Agregar usuarios desarrolladores a un clúster

Para conceder acceso al clúster a desarrolladores, haga lo siguiente:

1 Defina una función o ClusterRole para el usuario o el grupo y aplíquelos al clúster. Para obtener más información, consulte la documentación de Kubernetes.

2 Cree un RoleBinding o ClusterRoleBinding para el usuario o grupo y aplíquelo al clúster. Vea el ejemplo siguiente:

Ejemplo de RoleBinding

Para conceder acceso a un usuario o grupo de vCenter Single Sign-On, el asunto en RoleBinding debe contener uno de los siguientes valores para el parámetro `name`.

Tabla 11-1. Campos de usuario y grupo admitidos

Campo	Descripción
`sso:`*`USER-NAME@DOMAIN`*	Por ejemplo, un nombre de usuario local, como `sso:joe@vsphere.local`.
`sso:`*`GROUP-NAME@DOMAIN`*	Por ejemplo, un nombre de grupo de un servidor de directorio integrado con la instancia de vCenter Server, como `sso:devs@ldap.example.com`.

El siguiente ejemplo de RoleBinding enlaza el usuario local de vCenter Single Sign-On, llamado Joe, al objeto ClusterRole predeterminado denominado `edit`. Esta función permite el acceso de lectura/escritura a la mayoría de los objetos en un espacio de nombres, en este caso, el espacio de nombres `default`.

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: rolebinding-cluster-user-joe
  namespace: default
roleRef:
  kind: ClusterRole
```

```
  name: edit                             #Default ClusterRole
  apiGroup: rbac.authorization.k8s.io
subjects:
- kind: User
  name: sso:joe@vsphere.local            #sso:<username>@<domain>
  apiGroup: rbac.authorization.k8s.io
```

Configurar y administrar un Supervisor

12

Como administrador de vSphere, habilite un clúster de vSphere como Supervisor. Puede optar por crear el Supervisor con la pila de redes de vSphere o con VMware NSX® (NSX) como solución de red. Un clúster configurado con NSX admite la ejecución de un pod de vSphere y un clúster de Tanzu Kubernetes que se hayan creado a través de VMware Tanzu™ Kubernetes Grid™. Una instancia de Supervisor que se configura con la pila de redes de vSphere solo admite clústeres de Tanzu Kubernetes.

Después de habilitar el Supervisor, puede utilizar vSphere Client para administrar y supervisar el clúster.

Lea los siguientes temas a continuación:

- Reemplazar el certificado VIP para conectarse de forma segura al endpoint de API de Supervisor
- Integrar Tanzu Kubernetes Grid en el Supervisor con Tanzu Mission Control
- Configurar la CNI predeterminada para los clústeres de Tanzu Kubernetes Grid
- Cambiar el tamaño del plano de control de un Supervisor
- Cambiar la configuración del equilibrador de carga en un Supervisor configurado con redes VDS
- Agregar redes de cargas de trabajo a un Supervisor configurada con redes de VDS
- Cambiar la configuración de red de administración en un Supervisor
- Cambiar la configuración de red de carga de trabajo en un Supervisor configurada con redes de VDS
- Cambiar la configuración de red de carga de trabajo en un Supervisor configurado con NSX
- Configuración de los ajustes del proxy HTTP en vSphere IaaS control plane
- Configurar un IDP externo para usarlo con clústeres de servicio TKG
- Registrar un IDP externo con Supervisor
- Cambiar la configuración de almacenamiento en el Supervisor
- Transmisión de métricas de Supervisor a una plataforma de observación personalizada
- Modificar la lista de nombres DNS del plano de control del Supervisor

- Reenviar registros de Supervisor a sistemas de supervisión externos

Reemplazar el certificado VIP para conectarse de forma segura al endpoint de API de Supervisor

Como administrador de vSphere, puede reemplazar el certificado de la dirección IP virtual (virtual IP address, VIP) para conectarse de forma segura al endpoint de API de Supervisor con un certificado firmado por una CA en la que los hosts ya confíen. El certificado autentica el plano de control de Kubernetes para los ingenieros de desarrollo y operaciones, tanto en el inicio de sesión como en las interacciones posteriores con el Supervisor.

Requisitos previos

Compruebe que puede acceder a una CA que pueda firmar CSR. Para los ingenieros de desarrollo y operaciones, la CA debe estar instalada en su sistema como una raíz de confianza.

Para obtener más información sobre el certificado de Supervisor, consulte Certificado de CA de Supervisor.

Procedimiento

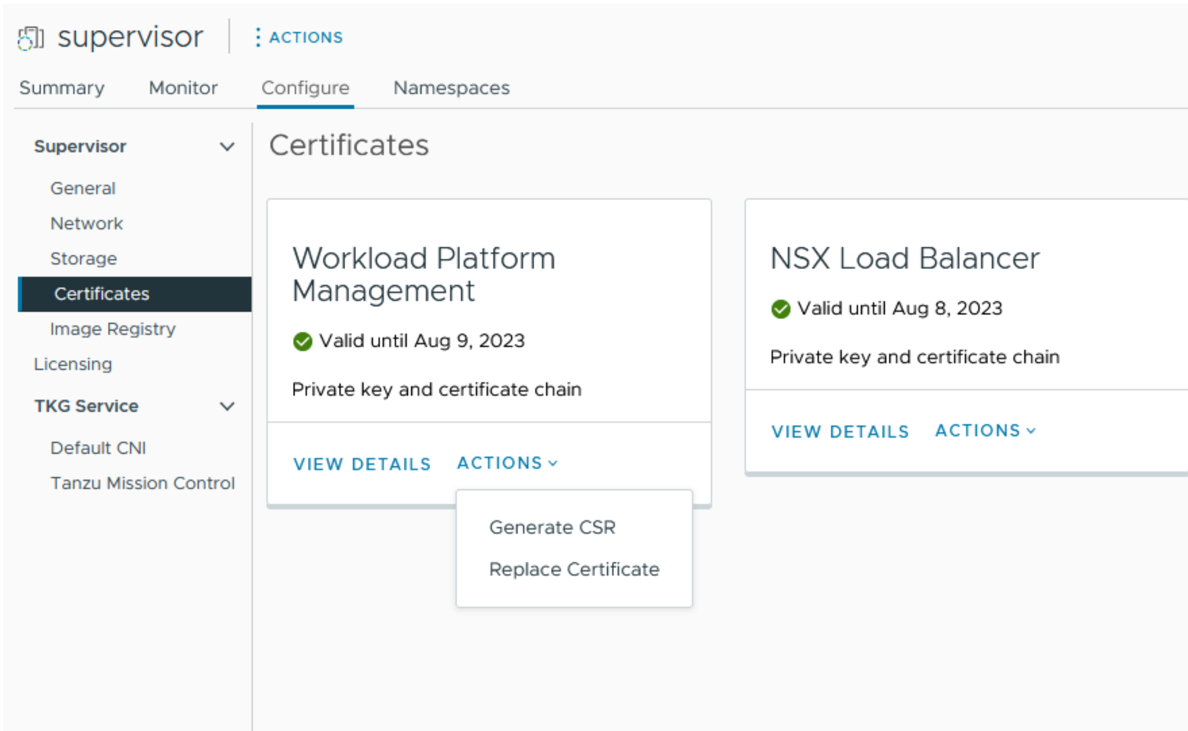
1 En vSphere Client, desplácese hasta **Administración de cargas de trabajo**.

2 Seleccione **Supervisores** y, a continuación, seleccione el Supervisor de la lista.

3 Haga clic en **Configurar** y seleccione **Certificados**.

4 En el panel **Plataforma de administración de cargas de trabajo**, seleccione **Acciones > Generar CSR**.

Figura 12-1. Reemplazando el certificado predeterminado de supervisor



5 Proporcione los detalles del certificado.

Nota Si utiliza un servicio de proveedor de identidad, también debe incluir la cadena de certificados completa. Sin embargo, la cadena no es necesaria para el tráfico HTTPS estándar.

6 Una vez que se genere la CSR, haga clic en **Copiar**.

7 Firme el certificado con una CA.

8 En el panel **Plataforma de administración de cargas de trabajo**, seleccione **Acciones > Reemplazar certificado**.

9 Cargue el archivo de certificado firmado y haga clic en **Reemplazar certificado**.

10 Valide el certificado en la dirección IP del plano de control de Kubernetes.

Por ejemplo, puede abrir la página de descarga de Herramientas de la CLI de Kubernetes para vSphere y confirmar que el certificado fue reemplazado correctamente desde el navegador. En un sistema Linux o Unix, también puede utilizar `echo | openssl s_client -connect https://ip:6443`.

Integrar Tanzu Kubernetes Grid en el Supervisor con Tanzu Mission Control

La instancia de Tanzu Kubernetes Grid que se ejecuta en el Supervisor se puede integrar con Tanzu Mission Control. Si lo hace, podrá aprovisionar y administrar los clústeres de Tanzu Kubernetes mediante Tanzu Mission Control.

Para obtener más información sobre Tanzu Mission Control, consulte Administrar el ciclo de vida de los clústeres de Tanzu Kubernetes. Para ver una demostración, vea el vídeo Tanzu Mission Control integrado con el servicio Tanzu Kubernetes Grid.

Ver el espacio de nombres de Tanzu Mission Control en el Supervisor

vSphere IaaS control plane v7.0.1 U1 y las versiones posteriores se distribuyen con un espacio de nombres de vSphere para Tanzu Mission Control. Este espacio de nombres se encuentra en el Supervisor donde se instala el agente de Tanzu Mission Control. Una vez se instala el agente, podrá aprovisionar y administrar los clústeres de Tanzu Kubernetes Grid mediante la interfaz web de Tanzu Mission Control.

1 Utilice complemento de vSphere para kubectl para autenticarse en Supervisor. Consulte Conectarse al Supervisor como usuario vCenter Single Sign-On.

2 Cambie el contexto al Supervisor, por ejemplo:

```
kubectl config use-context 10.199.95.59
```

3 Ejecute el siguiente comando para enumerar los espacios de nombres.

```
kubectl get ns
```

4 El espacio de nombres de vSphere que se proporciona para Tanzu Mission Control se identifica como `svc-tmc-cXX` (donde XX es un número).

5 Instale el agente de Tanzu Mission Control en este espacio de nombres. Consulte Instalar el agente de Tanzu Mission Control en el Supervisor.

Instalar el agente de Tanzu Mission Control en el Supervisor

Para integrar Tanzu Kubernetes Grid con Tanzu Mission Control, instale el agente en el Supervisor.

Nota El siguiente procedimiento requiere al menos vSphere 7.0 U3 con la versión 1.21.0 o posterior de Supervisor.

1 Mediante la interfaz web de Tanzu Mission Control, registre el Supervisor con Tanzu Mission Control. Consulte Registrar un clúster de administración en Tanzu Mission Control.

2 Mediante la interfaz web de Tanzu Mission Control, obtenga la URL de registro. Para ello, vaya a **Administración > Clústeres de administración**.

3 Abra un puerto de firewall en el entorno de vSphere IaaS control plane para el puerto que requiere Tanzu Mission Control (normalmente `443`). Consulte Conexiones salientes realizadas por las extensiones del agente de clúster.

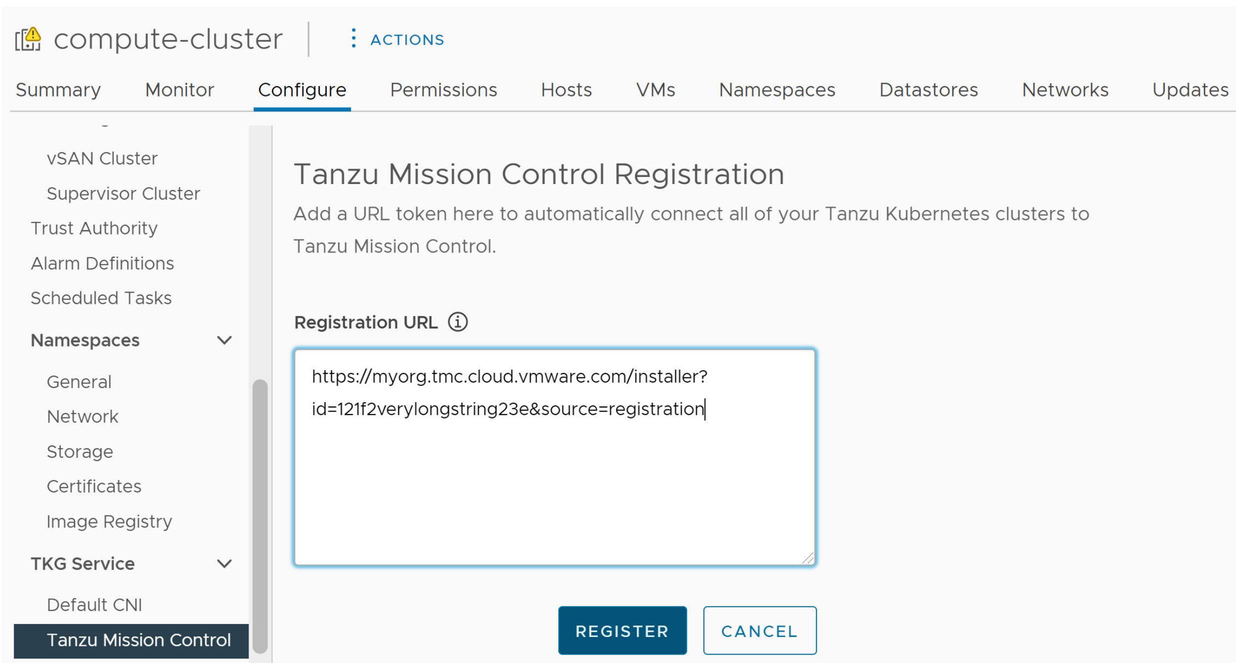
4 Inicie sesión en su entorno de vSphere IaaS control plane mediante vSphere Client.

5 Seleccione **Administración de cargas de trabajo** y seleccione el Supervisor.

6 Seleccione **Configurar** y seleccione **Servicio TKG > Tanzu Mission Control**.

7 Proporcione la URL de registro en el campo **URL de registro**.

8 Haga clic en **Registrar**.



Desinstale el agente de Tanzu Mission Control

Si quiere desinstalar el agente de Tanzu Mission Control de Supervisor, consulte Quitar de forma manual el agente de clústeres de un clúster de Supervisor en vSphere IaaS control plane.

Configurar la CNI predeterminada para los clústeres de Tanzu Kubernetes Grid

Como administrador vSphere, puede establecer la interfaz de red de contenedor (Container Network Interface, CNI) predeterminada para los clústeres de Tanzu Kubernetes.

CNI predeterminada

Tanzu Kubernetes Grid admite dos opciones de CNI para clústeres de Tanzu Kubernetes Grid: Antrea y Calico.

La CNI predeterminada definida por el sistema es Antrea. Para obtener más información sobre la configuración de la CNI predeterminada, consulte *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

Puede cambiar la CNI predeterminada mediante vSphere Client. Para establecer la CNI predeterminada, complete el siguiente procedimiento.

Precaución Cambiar la CNI predeterminada es una operación global. El valor predeterminado recién establecido se aplica a todos los clústeres nuevos creados por el servicio. Los clústeres existentes no se modifican.

---

1 Inicie sesión en su entorno de vSphere IaaS control plane mediante vSphere Client.

2 Seleccione **Administración de cargas de trabajo** y **Supervisores**.

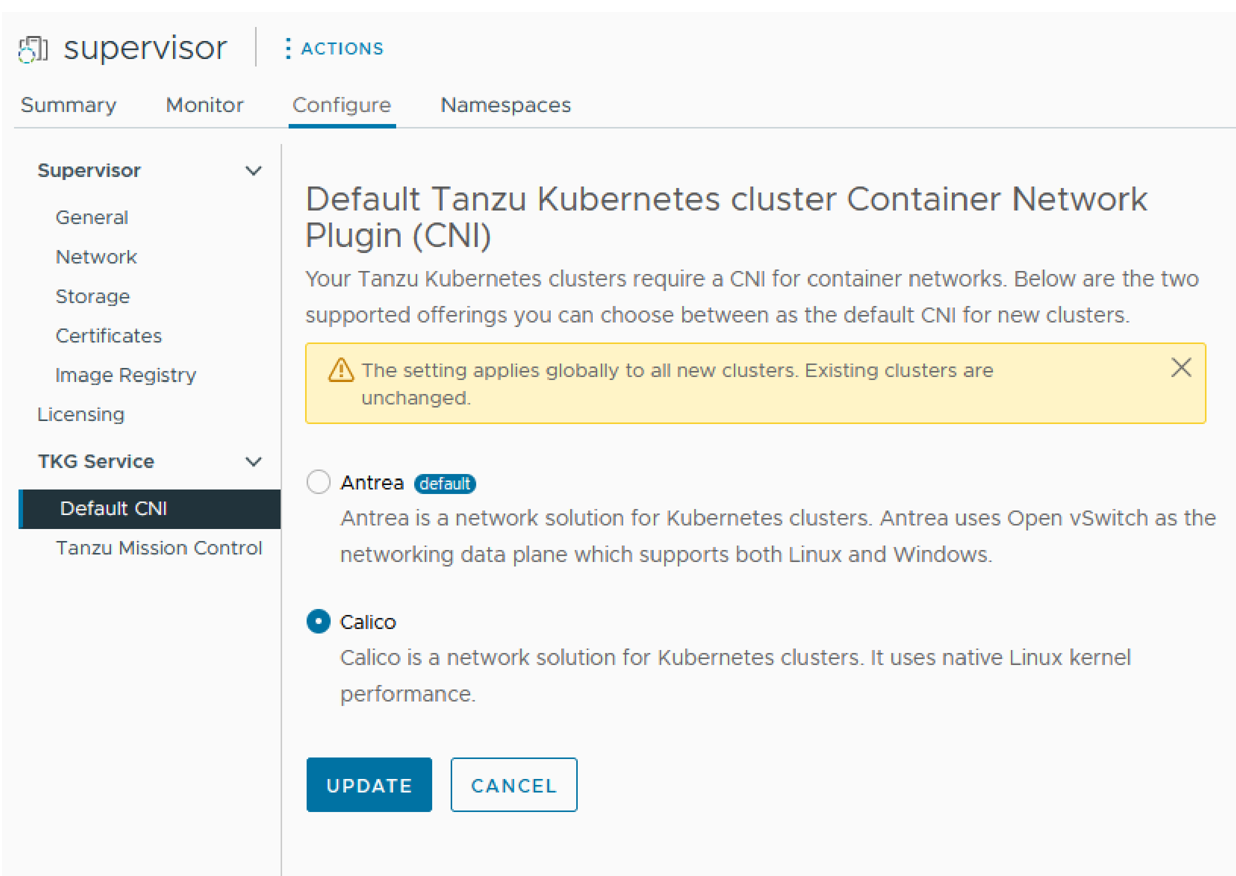
3 Seleccione la instancia de Supervisor de la lista.

4 Seleccione **Configurar** y **Servicio de TKG > CNI predeterminada**

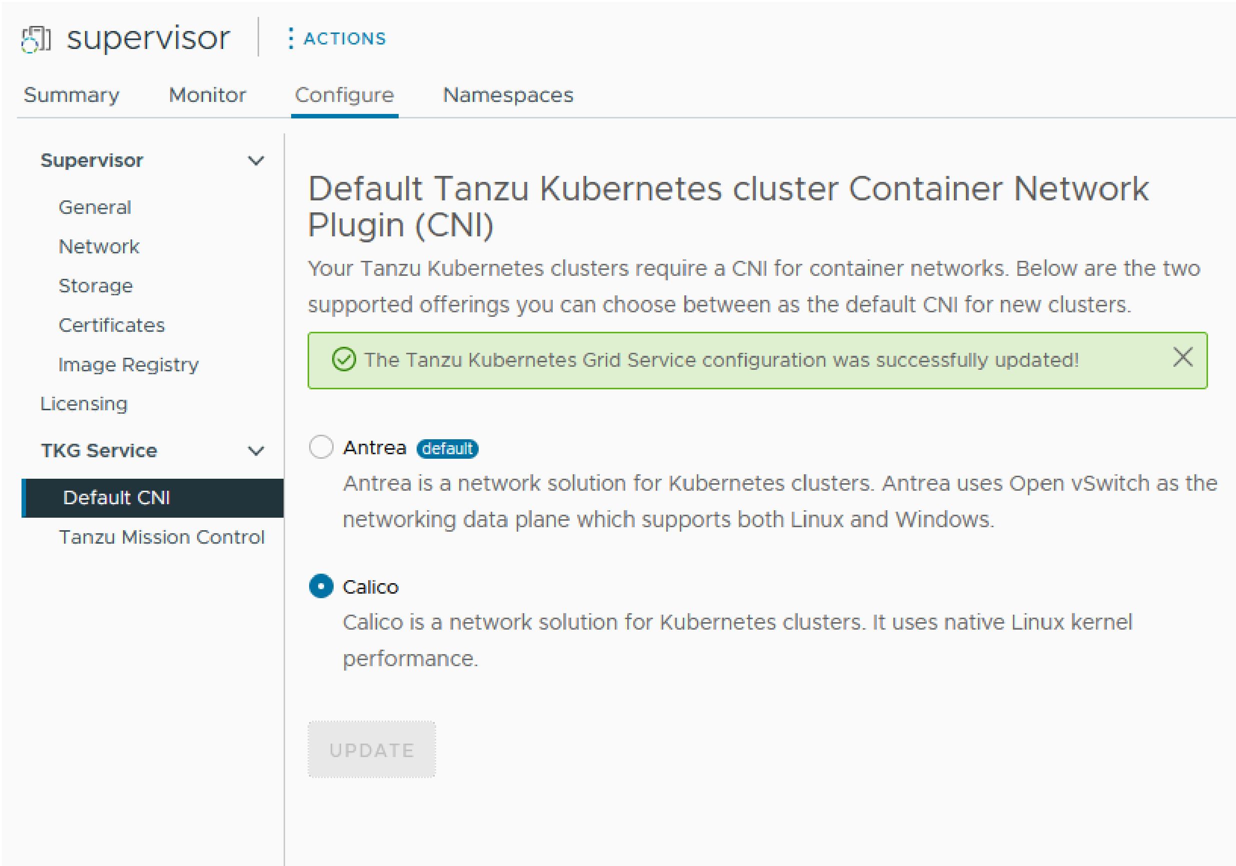
5 Elija la CNI predeterminada para los nuevos clústeres.

6 Haga clic en **Actualizar**.

La siguiente imagen muestra la selección de CNI predeterminada.



La siguiente imagen muestra cómo cambiar la selección de CNI de Antrea a Calico.



Cambiar el tamaño del plano de control de un Supervisor

Compruebe cómo cambiar el tamaño de las máquinas virtuales del plano de control de Kubernetes de un Supervisor en el entorno de vSphere IaaS control plane.

Requisitos previos

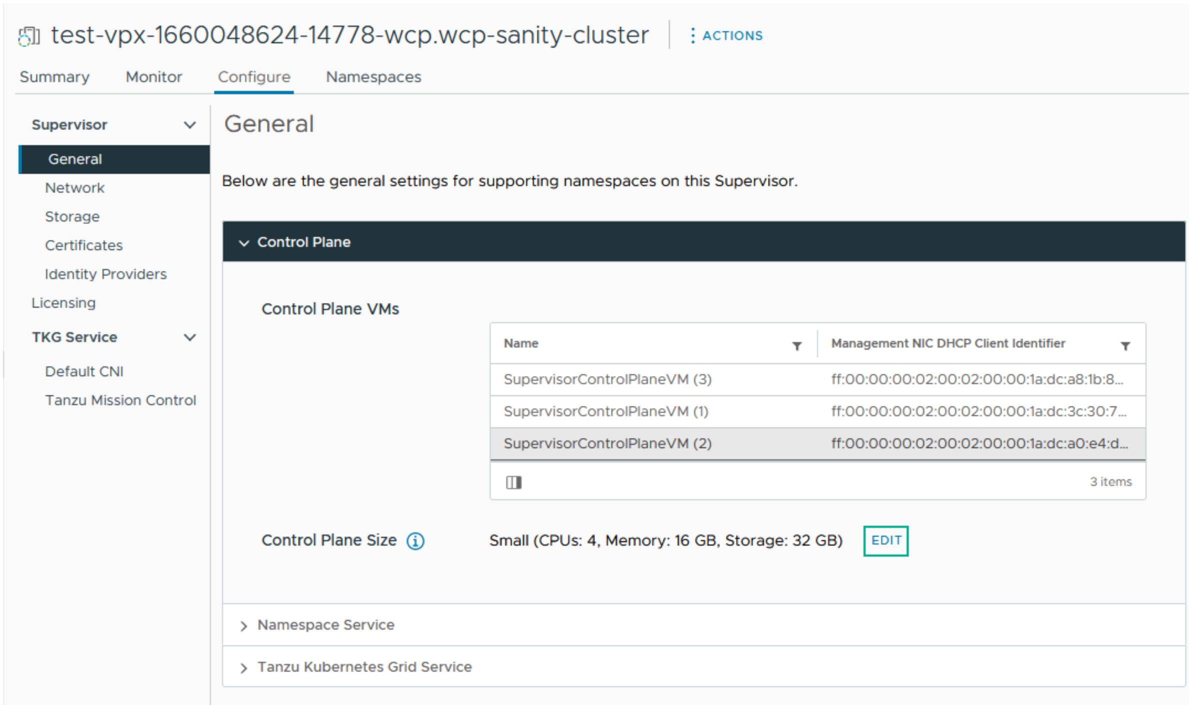
- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

Procedimiento

1. En vSphere Client, vaya a **Administración de cargas de trabajo**.
2. En **Supervisores**, seleccione el Supervisor.
3. Seleccione **Configurar** y **General**.

4 Expanda **Tamaño del plano de control**.

Figura 12-2. Configuración del plano de control del supervisor



5 Haga clic en **Editar** y seleccione un nuevo tamaño de plano de control en el menú desplegable.

Opción	Descripción
Muy pequeño	2 CPU, 8 GB de memoria, 32 GB de almacenamiento
Pequeño	4 CPU, 16 GB de memoria, 32 GB de almacenamiento
Mediano	8 CPU, 16 GB de memoria, 32 GB de almacenamiento
Grande	16 CPU, 32 GB de memoria, 32 GB de almacenamiento

Nota Una vez que seleccione el tamaño del plano de control, no podrá escalar horizontalmente. Por ejemplo, si ya configuró la opción Muy pequeño durante la activación de Supervisor, solo puede escalar verticalmente.

6 Haga clic en **Guardar**.

Solo puede escalar verticalmente el tamaño del plano de control.

Cambiar la configuración del equilibrador de carga en un Supervisor configurado con redes VDS

Consulte cómo cambiar la configuración del equilibrador de carga configurado con la pila de redes de VDS en el Supervisor. Puede cambiar la configuración, como el nombre de usuario y la

contraseña, agregar nuevos rangos de IP y actualizar el certificado utilizado con el equilibrador de carga.

Requisitos previos

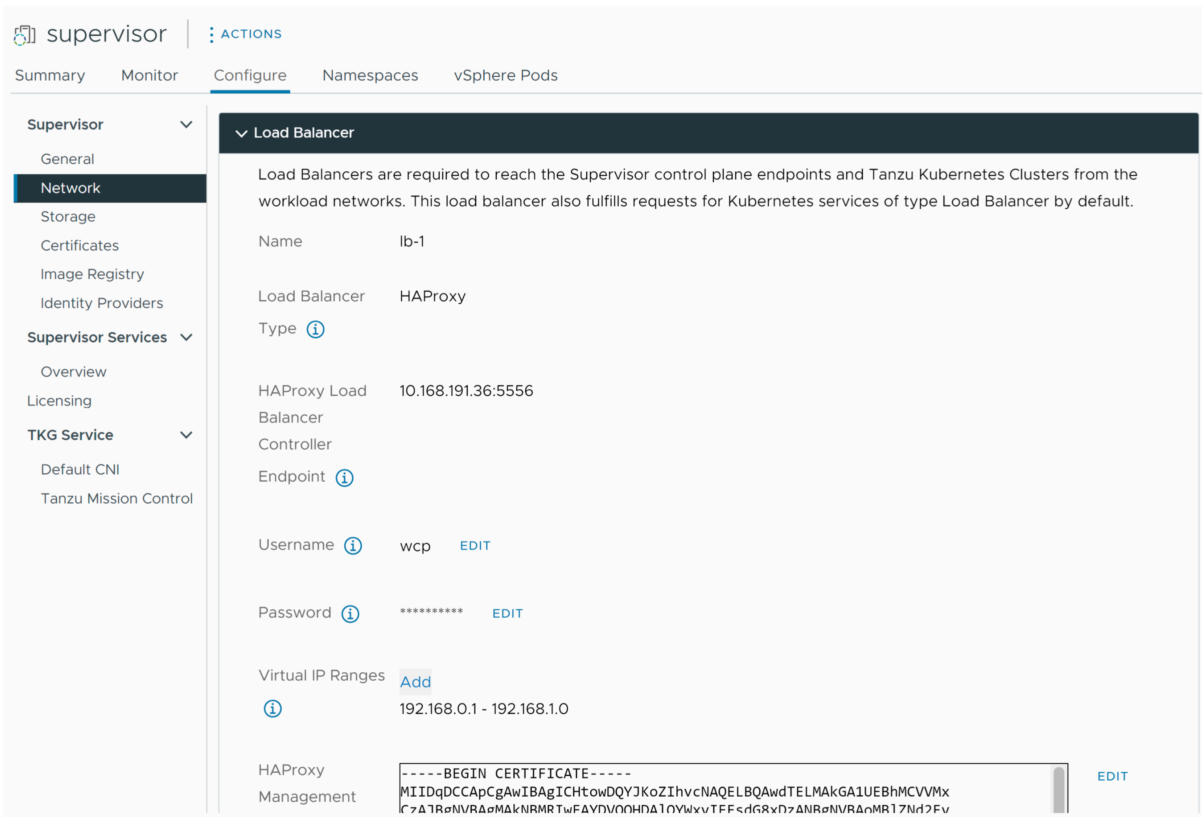
- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

Procedimiento

1 En vSphere Client, vaya a **Administración de cargas de trabajo**.

2 En **Supervisores**, seleccione el Supervisor y, a continuación, seleccione **Configurar**.

3 Seleccione **Red** y expanda **Red de carga de trabajo**.



Opción	Descripción
Configuración	Descripción
Nombre de usuario	Edite el nombre de usuario que utiliza el Supervisor para autenticarse con el endpoint del equilibrador de carga.
Contraseña	Cambie la contraseña que utiliza el Supervisor para autenticarse con el endpoint del equilibrador de carga.

Opción	Descripción
Rangos de direcciones IP virtuales	Agregue rangos de IP que sean un subconjunto del rango de CIDR de IP virtual que configuró inicialmente con el equilibrador de carga. **Nota** Solo puede agregar nuevos rangos de IP. No se pueden eliminar ni cambiar los rangos de IP existentes.
Certificado TLS	Cambie el certificado TLS que se utiliza para garantizar una conexión segura entre el Supervisor y el equilibrador de carga.

Agregar redes de cargas de trabajo a un Supervisor configurada con redes de VDS

Para un Supervisor configurada con la pila de redes vSphere, puede proporcionar aislamiento de Capa 2 para las cargas de trabajo de Kubernetes mediante la creación de redes de cargas de trabajo y su asignación a espacios de nombres. Las redes de cargas de trabajo proporcionan conectividad a los clústeres de Tanzu Kubernetes Grid en el espacio de nombres y están respaldadas por grupos de puertos distribuidos en el conmutador que está conectado a los hosts de Supervisor.

Para obtener más información sobre las topologías que se pueden implementar para el Supervisor, consulte Topología para un supervisor con redes de vSphere y NSX Advanced Load Balancer o Topologías para implementar el equilibrador de carga de HAProxy en *Planificación y conceptos del plano de control de IaaS de vSphere*.

Nota Si configuró Supervisor con un servidor DHCP que proporciona la configuración de redes para redes de cargas de trabajo, no podrá crear nuevas redes de cargas de trabajo después de la configuración de Supervisor.

Requisitos previos

- Cree un grupo de puertos distribuidos que respaldará la red de cargas de trabajo.
- Compruebe que el rango de IP que va a asignar a la red de cargas de trabajo sea único dentro de todas las instancias de Supervisor disponibles en su entorno.

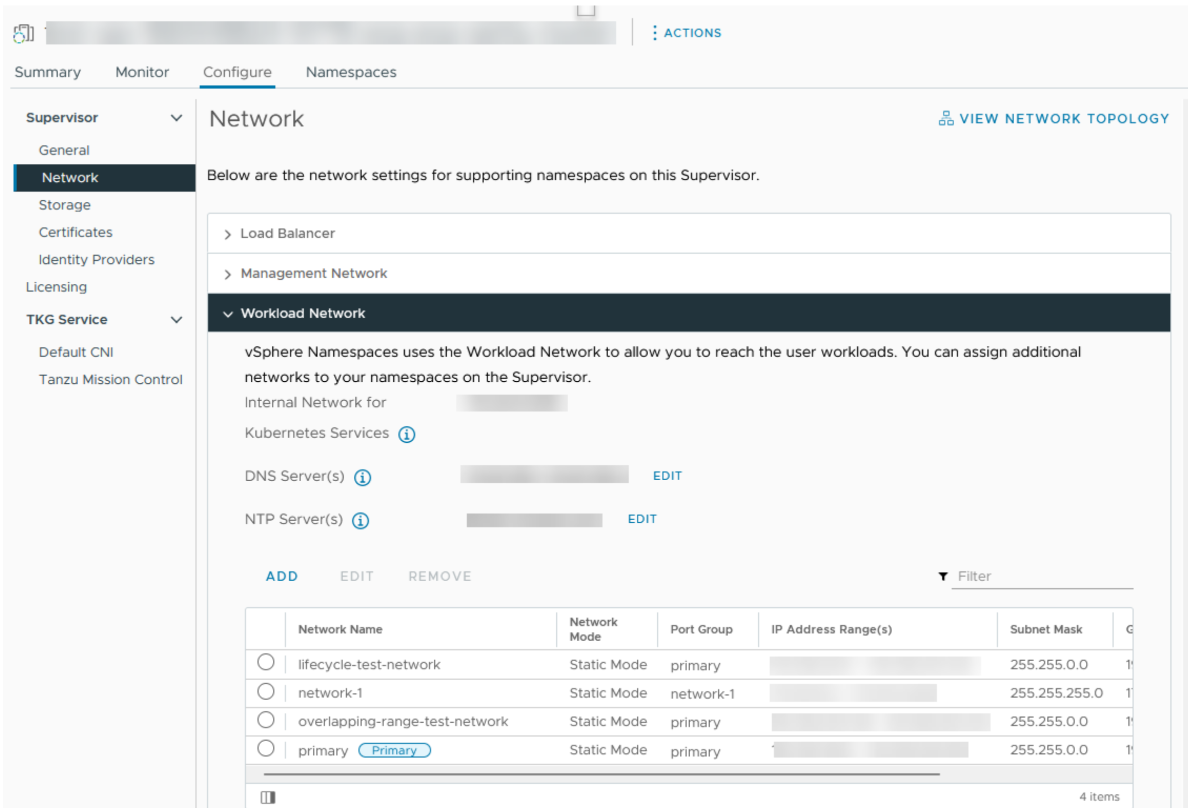
Procedimiento

1 En vSphere Client, vaya a **Administración de cargas de trabajo**.

2 En **Supervisores**, seleccione el Supervisor.

3 Seleccione **Configurar** y **Red**.

Figura 12-3. Agregar una red de carga de trabajo de supervisor



4 Seleccione **Red de carga de trabajo** y haga clic en **Agregar**.

Opción	Descripción
Grupo de puertos	Seleccione el grupo de puertos distribuidos que se asociará con esta red de cargas de trabajo. El conmutador vSphere Distributed Switch (VDS) configurado para la red de Supervisor contiene los grupos de puertos que se pueden seleccionar.
Nombre de red	El nombre de red que identifica la red de cargas de trabajo cuando se asigna a espacios de nombres. Este valor se rellena automáticamente a partir del nombre del grupo de puertos que seleccione, pero puede cambiarlo según corresponda.
Rangos de direcciones IP	Introduzca un rango de IP para asignar direcciones IP de nodos del clúster Tanzu Kubernetes Grid. El rango de IP debe estar en la subred indicada por la máscara de subred. **Nota** Debe utilizar rangos de direcciones IP únicos para cada red de cargas de trabajo. No configure los mismos rangos de direcciones IP para varias redes.

Opción	Descripción
Máscara de subred	Introduzca la dirección IP de la máscara de subred de la red en el grupo de puertos.
Puerta de enlace	Introduzca la puerta de enlace predeterminada para la red en el grupo de puertos. La puerta de enlace debe estar en la subred indicada por la máscara de subred. **Nota** No utilice la puerta de enlace que está asignada al equilibrador de carga de HAProxy.

5 Haga clic en **Agregar**.

Pasos siguientes

Asigne la red de cargas de trabajo recién creada a las instancias de espacio de nombres de vSphere.

Cambiar la configuración de red de administración en un Supervisor

Aprenda a actualizar la configuración de DNS y NTP en la red de administración de Supervisor en el entorno de vSphere IaaS control plane.

Requisitos previos

- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

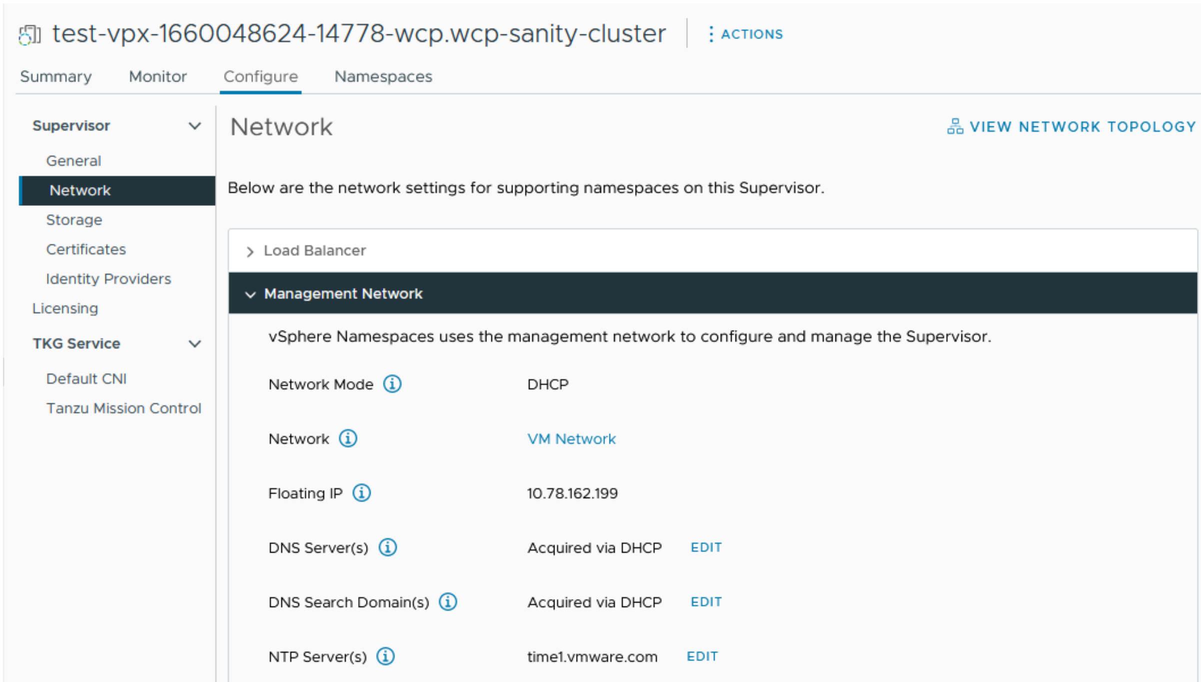
Procedimiento

1 En vSphere Client, seleccione **Administración de cargas de trabajo**.

2 En **Supervisores**, seleccione el Supervisor y, a continuación, seleccione **Configurar**.

3 Seleccione **Red** y expanda **Red de administración**.

Figura 12-4. Actualización de la configuración de red de administración del supervisor



4 Edite la configuración de DNS y NTP.

Opción	Descripción
Servidor(es) DNS	Introduzca las direcciones de los servidores DNS que utiliza en su entorno. Si el sistema vCenter Server está registrado con un FQDN, debe introducir las direcciones IP de los servidores DNS que utiliza con el entorno de vSphere para que el FQDN se pueda resolver en el Supervisor.
Dominio(s) de búsqueda de DNS	Introduzca los nombres de dominio que DNS busca dentro de los nodos del plano de control de Kubernetes, como `corp.local`, para que el servidor DNS pueda resolverlos.
Servidor(es) NTP	Introduzca las direcciones de los servidores NTP que utiliza en su entorno, si los hubiera.

Cambiar la configuración de red de carga de trabajo en un Supervisor configurada con redes de VDS

Consulte cómo cambiar la configuración del servidor NTP y DNS para las redes de cargas de trabajo de un Supervisor configurada con la pila de redes de VDS. Los servidores DNS que se configuran para las redes de cargas de trabajo son servidores DNS externos expuestos a cargas de trabajo de Kubernetes y resuelven los nombres de dominio predeterminados que se alojan fuera del Supervisor.

Requisitos previos

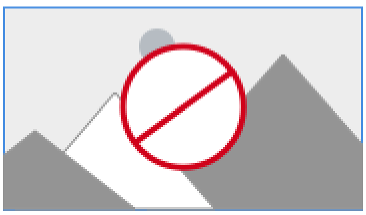
- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

Procedimiento

1 En vSphere Client, seleccione **Administración de cargas de trabajo**.

2 En **Supervisores**, seleccione el Supervisor y, a continuación, seleccione **Configurar**.

3 Seleccione **Red** y expanda **Red de carga de trabajo**.



Nota No se puede eliminar una red de cargas de trabajo que ya esté asignada a un espacio de nombres de vSphere. Si necesita eliminar una red de cargas de trabajo, debe eliminar todos los espacios de nombres de vSphere asociados a esa red. Tampoco puede editar ni eliminar la red de cargas de trabajo principal.

4 Edite la configuración del servidor DNS.

Introduzca las direcciones de los servidores DNS que pueden resolver los nombres de dominio de los componentes de administración de vSphere, como por ejemplo vCenter Server.

Por ejemplo, `10.142.7.1`.

Al introducir la dirección IP del servidor DNS, se agrega una ruta estática a cada máquina virtual del plano de control. Esto indica que el tráfico a los servidores DNS pasa por la red de cargas de trabajo.

Si los servidores DNS que especifica se comparten entre la red de administración y la red de cargas de trabajo, las búsquedas de DNS en las máquinas virtuales del plano de control se enrutan a través de la red de cargas de trabajo después de la configuración inicial.

5 Edite la configuración de NTP según sea necesario.

6 Edite la configuración de red de cargas de trabajo.

a Seleccione una red de cargas de trabajo y haga clic en **Editar**.

b Haga clic en **Agregar** junto a **Rango(s) de direcciones IP** para agregar nuevos rangos de IP que se utilizarán con las cargas de trabajo en esa red.

Los rangos de IP deben estar en la subred indicada por la máscara de subred.

Nota Los rangos de IP que agregue no deben superponerse con las direcciones IP virtuales de la configuración de red de front-end del equilibrador de carga.

Cambiar la configuración de red de carga de trabajo en un Supervisor configurado con NSX

Aprenda a cambiar la configuración de red para el servidor DNS, las redes de espacio de nombres, la entrada y la salida de un Supervisor configurado para NSX como la pila de redes.

Requisitos previos

- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

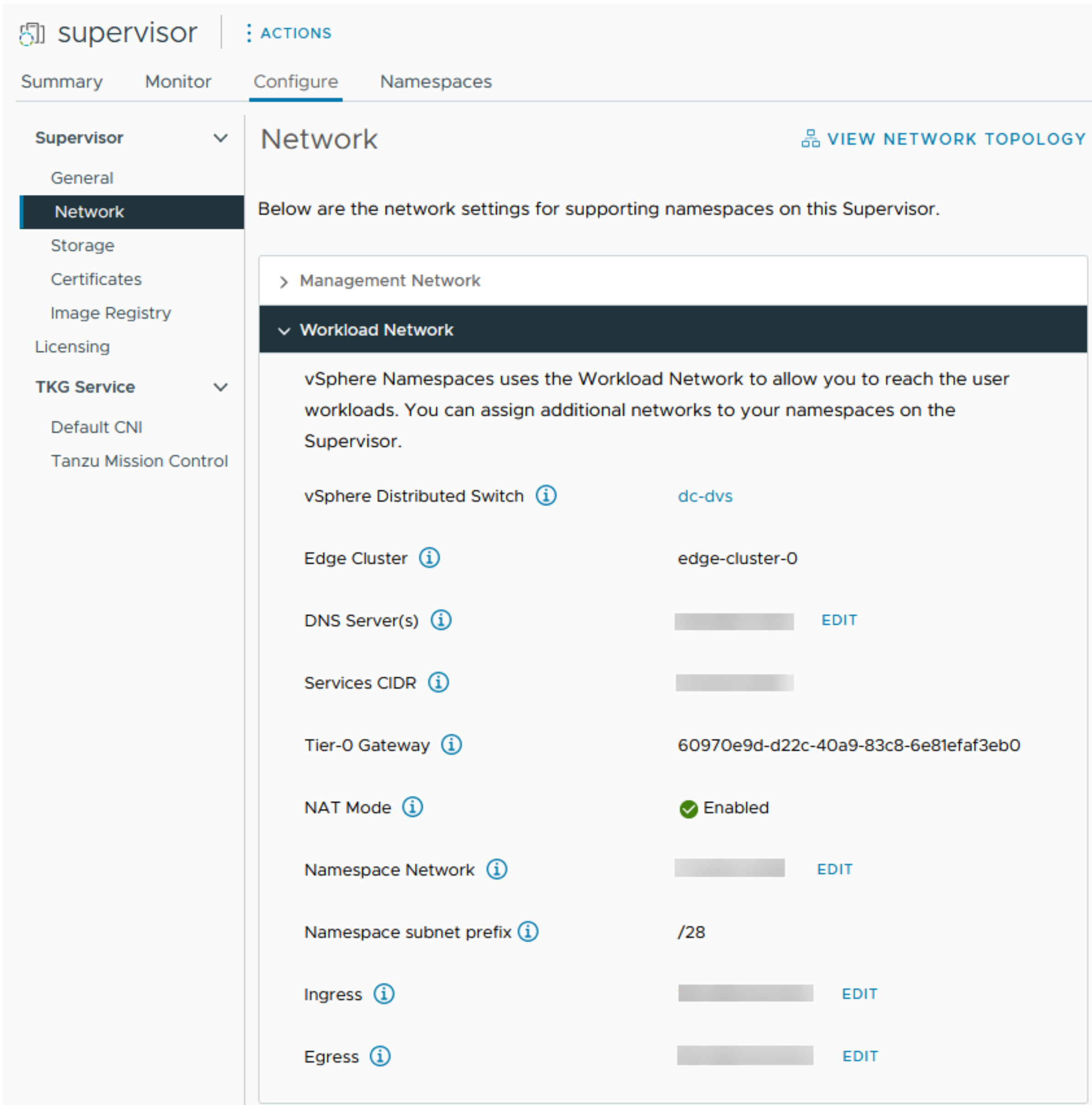
Procedimiento

1 En vSphere Client, desplácese hasta **Administración de cargas de trabajo**.

2 En **Supervisores**, seleccione el Supervisor y, a continuación, seleccione **Configurar**.

3 Seleccione **Red** y expanda **Red de carga de trabajo**.

Figura 12-5. Actualización de la configuración de red de carga de trabajo del supervisor



4 Cambie la configuración de redes según sea necesario.

Opción	Descripción
Servidor(es) DNS	Introduzca las direcciones de los servidores DNS que pueden resolver los nombres de dominio de los componentes de administración de vSphere, como por ejemplo vCenter Server. Por ejemplo, `10.142.7.1`. Cuando se introduce la dirección IP del servidor DNS, se agrega una ruta estática a cada máquina virtual del plano de control. Esto indica que el tráfico a los servidores DNS pasa por la red de cargas de trabajo. Si los servidores DNS que especifica se comparten entre la red de administración y la red de cargas de trabajo, las búsquedas de DNS en las máquinas virtuales del plano de control se enrutan a través de la red de cargas de trabajo después de la configuración inicial.
Red de espacio de nombres	Introduzca una anotación CIDR para cambiar el rango de IP de las cargas de trabajo de Kubernetes que están asociadas a los segmentos de espacio de nombres del Supervisor. Si el modo NAT no está configurado, este rango de CIDR de IP debe ser una dirección IP enrutable.
Ingreso	Introduzca una anotación CIDR para cambiar el rango de IP de entrada de los servicios de Kubernetes. Este rango se utiliza para los servicios de tipo equilibrador de carga y entrada. Para los clústeres deTanzu Kubernetes Grid, la publicación de servicios a través del equilibrador de carga ServiceType también obtendrá las direcciones IP de este bloque CIDR de IP. **Nota** Solo puede agregar los CIDR a los campos de red de entrada y carga de trabajo, pero no puede editar ni eliminar los existentes.
Egreso	Introduzca una anotación CIDR para asignar direcciones IP para la Traducción de Direcciones de Red de Origen (Source Network Address Translation, SNAT) para el tráfico que sale del Supervisor para acceder a servicios externos. Solo se asigna una dirección IP de egreso para cada espacio de nombres en el Supervisor. La IP de salida es la dirección IP que los pods de vSphere en el espacio de nombres concreto usan para comunicarse fuera de NSX.

Configuración de los ajustes del proxy HTTP en vSphere IaaS control plane

Consulte cómo configurar los ajustes del proxy HTTP en los clústeres de Supervisor y TKG, y cuál es el flujo de trabajo para configurar un proxy cuando se registran los clústeres de Supervisor y TKG con Tanzu Mission Control.

Puede configurar un proxy en el Supervisor mediante vSphere Client, la API de administración de clústeres o los comandos de la DCLI. Puede utilizar un proxy si necesita controlar el tráfico de contenedor o la extracción de imágenes desde redes externas al Supervisor. Para los Supervisores locales que registre como clústeres de administración en Tanzu Mission Control, utilice un proxy HTTP para la extracción de imágenes y el tráfico de contenedor.

Configurar los ajustes de proxy en Supervisores de vSphere 7.0 Update 3 y versiones posteriores creados recientemente

Para los Supervisores creados recientemente en un entorno de vSphere 7.0 Update 3 y posterior, la configuración de proxy HTTP se hereda de vCenter Server. Independientemente de si crea Supervisores antes o después de configurar los ajustes del proxy HTTP en vCenter Server, los clústeres heredan la configuración.

Consulte Configurar los ajustes de DNS, dirección IP y proxy para obtener información sobre cómo configurar los ajustes del proxy HTTP en vCenter Server.

También puede anular la configuración del proxy HTTP heredado en Supervisores individuales a través de vSphere Client, la API de administración de clústeres o la DCLI.

Dado que heredar la configuración del proxy de vCenter Server es la configuración predeterminada para los Supervisores de vSphere 7.0.3 creados recientemente, también puede utilizar la API de administración del clúster o DCLI para no heredar ninguna configuración de proxy HTTP en caso de que los Supervisores no requieran un proxy, pero vCenter Server sigue requiriéndolo.

Configurar los ajustes de proxy en Supervisores actualizados a vSphere 7.0 Update 3 y versiones posteriores

Si actualizó Supervisores a vSphere 7.0 Update 3 y posterior, la configuración de proxy HTTP de vCenter Server no se hereda automáticamente. En ese caso, los ajustes de proxy de los Supervisores se pueden configurar mediante vSphere Client, la API `vcenter/namespace-management/clusters` o la línea de comandos de la DCLI.

Configurar un proxy HTTP para clústeres de TKG en vSphere IaaS control plane

Utilice uno de los siguientes métodos para configurar un proxy para los clústeres de Tanzu Kubernetes en vSphere IaaS control plane:

- Configure los ajustes de proxy para clústeres de TKG individuales. Consulte Parámetros de configuración para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de Tanzu Kubernetes Grid Service. Para ver un ejemplo de YAML de configuración, consulte Ejemplo de YAML para aprovisionar un clúster personalizado de Tanzu Kubernetes mediante la API v1alpha2 de Tanzu Kubernetes Grid Service.
- Cree una configuración de proxy global que se aplicará a todos los clústeres de TKG. Consulte Parámetros de configuración para la API v1alpha2 de Tanzu Kubernetes Grid Service.

Nota Si utiliza Tanzu Mission Control para administrar los clústeres de TKG, no es necesario configurar los ajustes de proxy a través del archivo YAML del clúster en vSphere IaaS control plane. Puede configurar los ajustes de proxy cuando agregue los clústeres de TKG como clústeres de carga de trabajo a Tanzu Mission Control.

Configurar el proxy HTTP en el Supervisor mediante vSphere Client

Consulte cómo configurar el proxy HTTP en el Supervisor mediante vSphere Client. Puede anular la configuración del proxy que se hereda de vCenter Server en los Supervisores individuales o seleccionar no utilizar ninguna configuración de proxy.

Requisitos previos

- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

Procedimiento

1. En vSphere Client, desplácese hasta **Administración de cargas de trabajo**.
2. En **Supervisores**, seleccione el Supervisor y, a continuación, seleccione **Configurar**.
3. Seleccione **Red**, expanda **Configuración de proxy** y haga clic en **Editar**.
4. Seleccione Configurar los ajustes de proxy en Supervisor e introduzca la configuración de proxy.

Opción	Descripción
Certificado TLS	El paquete de CA raíz de TLS del proxy que se utiliza para comprobar los certificados del proxy. Introduzca el paquete en texto sin formato.
Hosts y direcciones IP excluidos del proxy	Una lista separada por comas de direcciones IPv4, FQDN o nombres de dominio que no requieren el servidor proxy y a los que se puede acceder directamente.
Configuración de HTTPS	Configuración de HTTPS, como URL, puerto, nombre de usuario y contraseña.
Configuración de HTTP	Configuración de HTTP, como URL, puerto, nombre de usuario y contraseña.

5. Haga clic en **Aceptar**.

Resultados

La configuración de proxy que determinó en este Supervisor reemplaza la configuración heredada de vCenter Server.

Usar la API de administración de clústeres y la DCLI para configurar el proxy HTTP en Supervisores

Puede configurar los ajustes del proxy del Supervisor a través de la API `vcenter/namespace-management/clusters` o la DCLI.

La API proporciona tres opciones para la configuración de proxy en el Supervisor:

Configuración de API	Supervisores de vSphere 7.0.3 y versiones posteriores creados recientemente	Supervisores actualizados a vSphere 7.0.3 y versiones posteriores
`VC_INHERITED`	Este es el ajuste predeterminado para los nuevos Supervisores y no es necesario utilizar la API para configurar los ajustes de proxy de los Supervisores. Solo puede configurar los ajustes de proxy de los vCenter Server a través de su interfaz de administración.	Utilice esta opción para insertar la configuración de proxy HTTP en los Supervisores actualizados a vSphere 7.0.3 y posterior.
`CLUSTER_CONFIGURED`	Utilice esta opción para anular la configuración de proxy HTTP heredada de vCenter Server en uno de los siguientes casos: ■ Se requiere un Supervisor en una subred diferente a vCenter Server y se requiere un servidor proxy diferente. ■ El servidor proxy utiliza paquetes de CA personalizados.	Utilice esta opción para configurar el proxy HTTP para Supervisores individuales actualizados a vSphere 7.0.3 y posterior en uno de los siguientes casos: ■ No se puede utilizar el proxy de vCenter Server porque Supervisor reside en una subred diferente a vCenter Server y se requiere un servidor proxy diferente. ■ El servidor proxy utiliza paquetes de CA personalizados.
`NONE`	Utilice esta opción cuando Supervisor tenga conectividad directa a Internet mientras vCenter Server requiera un proxy. El ajuste NINGUNO impide que vCenter Server herede la configuración de proxy de los Supervisores.	

Para establecer un proxy HTTP para un Supervisor o modificar la configuración existente, utilice los siguientes comandos en una sesión SSH con vCenter Server :

```
vc_address=<IP address>
cluster_id=domain-c<number>
session_id=$(curl -ksX POST --user '<SSO user name>:<password>' https://$vc_address/api/
session | xargs -t)
curl -k -X PATCH -H "vmware-api-session-id: $session_id" -H "Content-Type: application/
json" -d '{ "cluster_proxy_config": { "proxy_settings_source": "CLUSTER_CONFIGURED",
"http_proxy_config":"<proxy_url>" } }' https://$vc_address/api/vcenter/namespace-management/
clusters/$cluster_id
```

Solo es necesario transferir el `domain_c<number>` del identificador de clúster completo. Por ejemplo, tome `domain-c50` del siguiente identificador de clúster: `ClusterComputeResource:domain-c50:5bbb510f-759f-4e43-96bd-97fd703b4edb`.

Cuando utilice la configuración de `VC_INHERITED` o `NONE`, omita `"http_proxy_config:<proxy_url>"` en el comando.

Para utilizar un paquete de CA personalizado, agregue `"tlsRootCaBundle": "<TLS_certificate>"` al comando proporcionando el certificado de CA de TSL en texto sin formato.

Para la configuración del proxy HTTPS, use el siguiente comando:

```
curl -k -X PATCH -H "vmware-api-session-id: $session_id"
-H "Content-Type: application/json" -d '{ "cluster_proxy_config":
{ "proxy_settings_source": "CLUSTER_CONFIGURED", "https_proxy_config":"<proxy_url>" } }'
https://$vc_address/api/vcenter/namespace-management/clusters/$cluster_id
```

Usar DCLI para configurar los ajustes del proxy HTTP en Supervisores

Puede usar el siguiente comando DCLI para configurar los ajustes del proxy HTTP para Supervisores mediante la opción `CLUSTER_CONFIGURED`.

```
<dcli> namespacemanagement clusters update --cluster domain-c57 --cluster-proxy-config-http-
proxy-config <proxy URL> --cluster-proxy-config-https-proxy-config <proxy URL> --cluster-
proxy-config-proxy-settings-source CLUSTER_CONFIGURED
```

Configurar los ajustes del proxy HTTP en los clústeres de Supervisor y TKG para Tanzu Mission Control

Para configurar un proxy HTTP en los Supervisores que desea registrar como clústeres de administración con Tanzu Mission Control, siga los pasos que se indican a continuación:

1 En vSphere, configure el proxy HTTP en Supervisores heredando la configuración del proxy HTTP de vCenter Server o configurando los ajustes del proxy en Supervisores individuales a través de vSphere Client, las API de clústeres de administración de espacios de nombres o la línea de comandos de la DCLI.

2 En Tanzu Mission Control, cree un objeto de configuración de proxy mediante los ajustes de proxy que configuró para los Supervisores en vSphere IaaS control plane. Consulte Crear un objeto de configuración de proxy para un clúster de Tanzu Kubernetes Grid Service.

3 En Tanzu Mission Control, utilice este objeto de configuración de proxy cuando registre Supervisores como clúster de administración. Consulte Registrar un clúster de administración con Tanzu Mission Control y Completar el registro de un clúster supervisor.

Para configurar un proxy HTTP para clústeres de TKG que aprovisione o agregue como clústeres de carga de trabajo en Tanzu Mission Control:

1 Cree un objeto de configuración de proxy con la configuración de proxy que desea utilizar con clústeres de Tanzu Kubernetes. Consulte Crear un objeto de configuración de proxy para un clúster de Tanzu Kubernetes Grid Service.

2 Utilice ese objeto de configuración de proxy cuando aprovisione o agregue clústeres de Tanzu Kubernetes como clústeres de carga de trabajo. Consulte Aprovisionar un clúster y Agregar un clúster de carga de trabajo a Tanzu Mission Control Management

Configurar un IDP externo para usarlo con clústeres de servicio TKG

Es posible configurar Supervisor con cualquier proveedor de identidad (Identity Provider, IDP) compatible con OIDC, como Okta. Para completar la integración, configure el IDP con la URL de devolución de llamada para Supervisor.

Proveedores de OIDC externos compatibles

Es posible configurar el Supervisor con cualquier proveedor de identidad compatible con OIDC. La tabla enumera los más comunes y proporciona vínculos a las instrucciones de configuración.

IDP externo	Configuración
Okta	Ejemplo de configuración de OIDC mediante Okta Consulte también Configurar Okta como proveedor de OIDC para Pinniped.
Workspace ONE	Configurar Workspace ONE Access como proveedor de OIDC para Pinniped
Dex	Configurar Dex como proveedor de OIDC para Pinniped
GitLab	Configurar GitLab como proveedor de OIDC para Pinniped
Google OAuth	Uso de Google OAuth 2

Configurar el IDP con la URL de devolución de llamada para el Supervisor

El Supervisor actúa como un cliente de OAuth 2.0 para el proveedor de identidad externo. La URL de devolución de llamada del Supervisor es la URL de redireccionamiento que se utiliza para configurar el IDP externo. La URL de devolución de llamada tiene el formato *https://SUPERVISOR-VIP/wcp/pinniped/callback*.

Nota Al realizar el registro de IDP, es posible que la URL de devolución de llamada se llame "URL de redireccionamiento" en el proveedor de OIDC que está configurando.

Al configurar el proveedor de identidad externo para usarlo con TKG en Supervisor, proporcione al proveedor de identidad externo la **URL de devolución de llamada** que se proporciona en vCenter Server en la pantalla **Administración de cargas de trabajo > Supervisores > Configurar > Proveedores de identidad**.

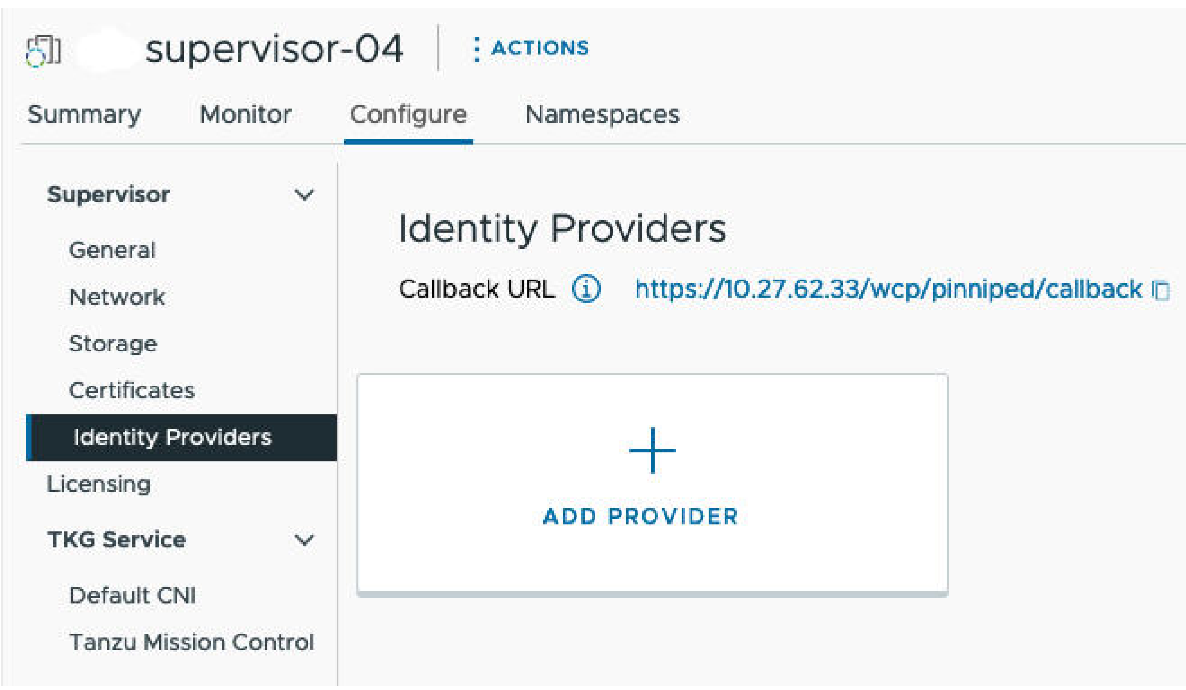
Ejemplo de configuración de OIDC mediante Okta

Okta permite a los usuarios iniciar sesión en las aplicaciones mediante el protocolo OpenID Connect. Cuando se configura Okta como proveedor de identidad externo para Tanzu Kubernetes Grid en Supervisor, los pods Pinniped en Supervisor y en clústeres de Tanzu Kubernetes Grid controlan el acceso de los usuarios a los espacios de nombres de vSphere y los clústeres de cargas de trabajo.

1 Copie la URL de devolución de llamada del proveedor de identidad para el que necesita crear una conexión de OIDC entre Okta y vCenter Server.

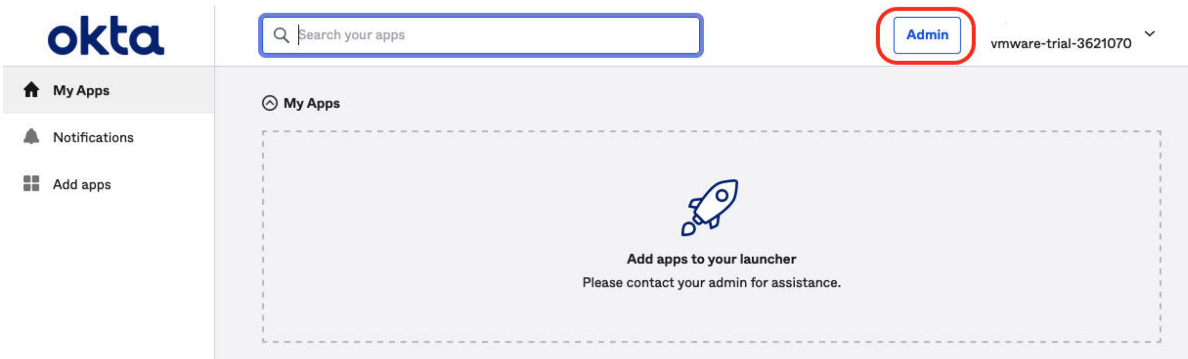
   Con vSphere Client, obtenga la URL de devolución de llamada del proveedor de identidad en **Administración de cargas de trabajo > Supervisores > Configurar > Proveedores de identidad**. Copie esta URL en una ubicación temporal.

   Figura 12-6. URL de devolución de llamada de IDP



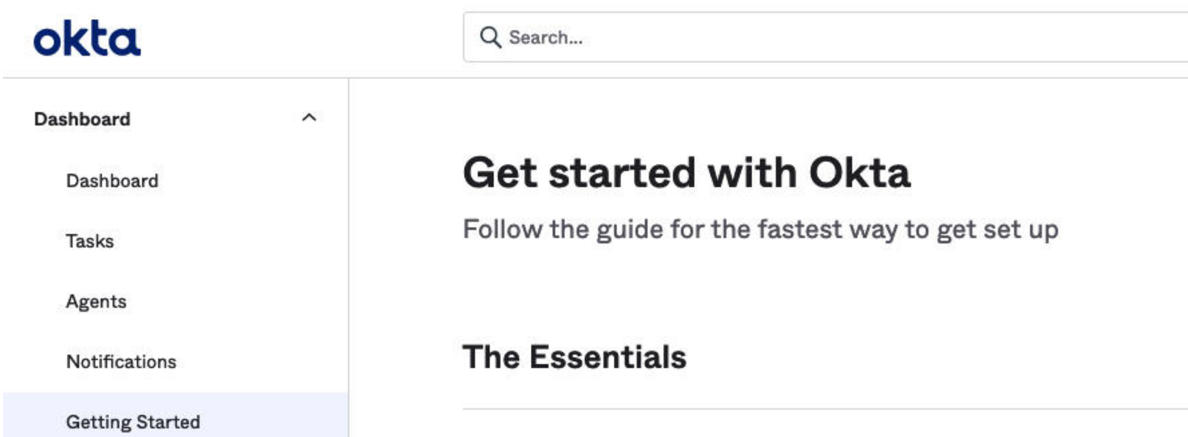
2 Inicie sesión en la cuenta de Okta de su organización o cree una cuenta de prueba en https://www.okta.com/. Haga clic en el botón **Admin** para abrir la consola administrativa de Okta.

Figura 12-7. Consola administrativa de Okta



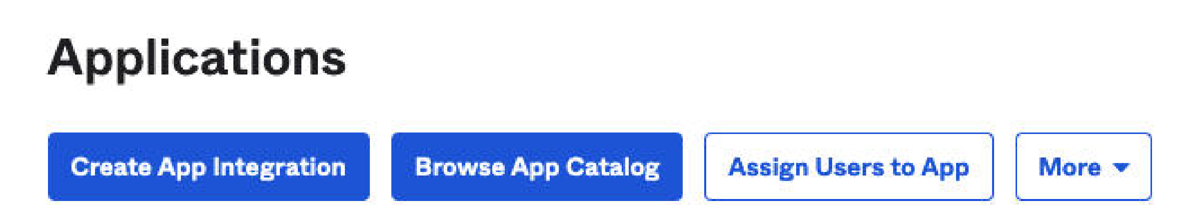
3 En la página de introducción de la consola administrativa, desplácese hasta **Applications (Aplicaciones) > Applications (Aplicaciones)**.

Figura 12-8. Introducción a Okta



4 Seleccione la opción para **crear una integración de aplicaciones**.

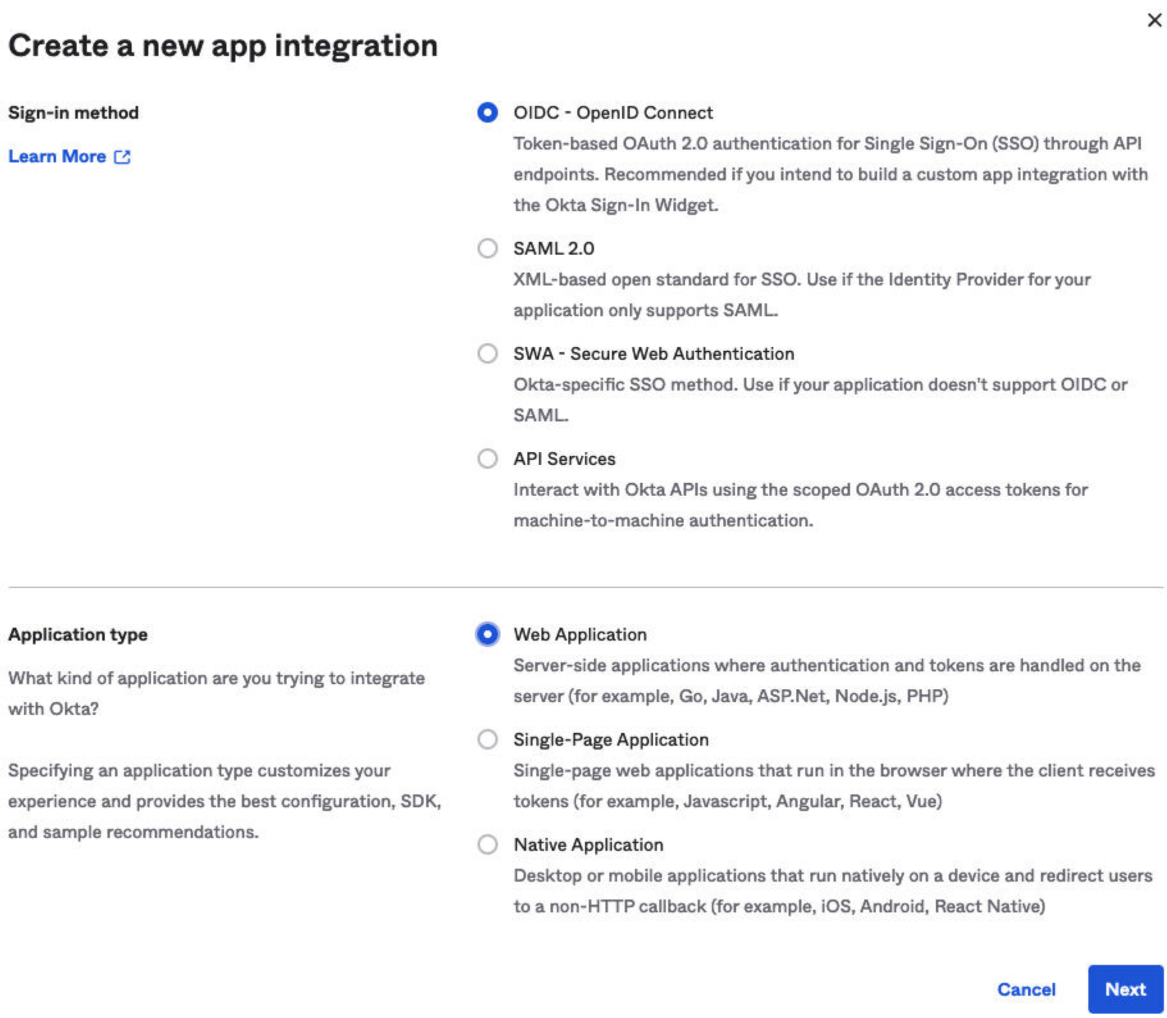
Figura 12-9. Crear integración de aplicaciones de Okta



5 Cree la nueva integración de aplicaciones.

- Establezca el método de inicio de sesión en **OIDC - OpenID Connect**.
- Establezca el tipo de aplicación en una **aplicación web**.

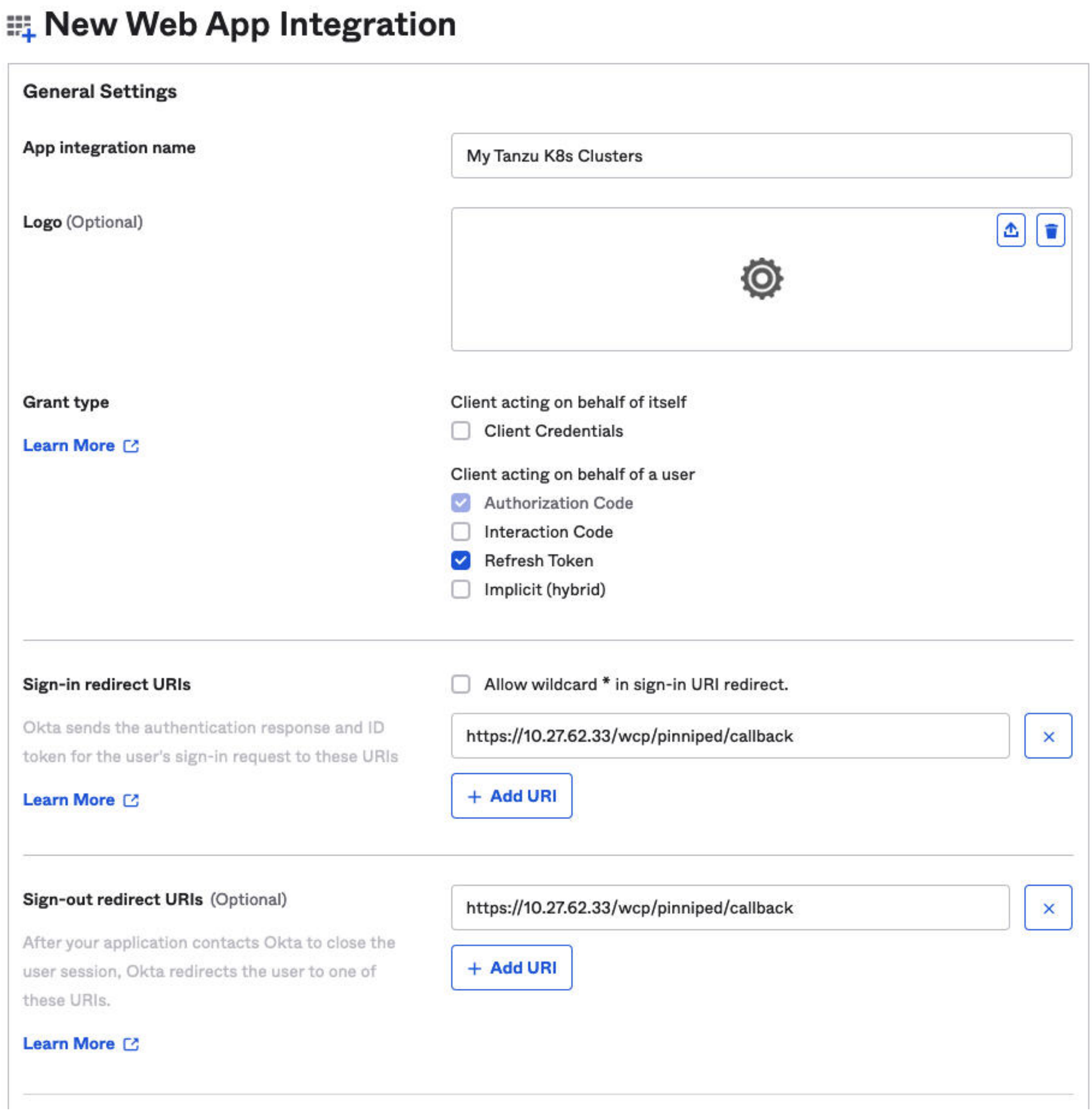
Figura 12-10. Método de inicio de sesión de Okta y tipo de aplicación



6 Configure los detalles de integración de la aplicación web de Okta.

- Proporcione un **nombre para la integración de aplicaciones**, que sea una cadena definida por el usuario.
- Especifique el **tipo de concesión**: se debe seleccionar **Authorization Code** (Código de autorización) y **Refresh Token** (Token de referencia).
- URI de redirección de inicio de sesión: introduzca la URL de devolución de llamada del proveedor de identidad que copió de Supervisor (vea el paso 1), como https://10.27.62.33/wcp/pinnipend/callback.
- URI de redirección de cierre de sesión: introduzca la URL de devolución de llamada del proveedor de identidad que copió de Supervisor (vea el paso 1), como https://10.27.62.33/wcp/pinnipend/callback.

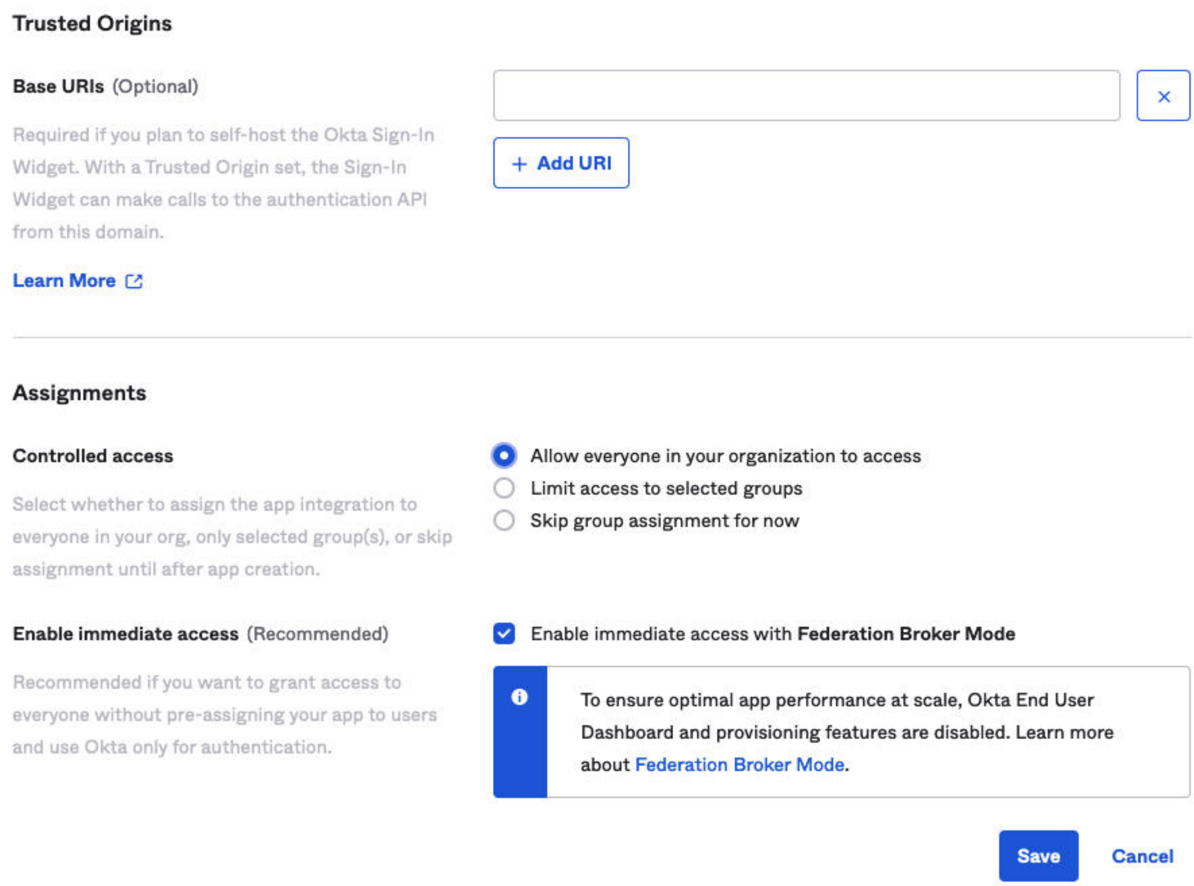
Figura 12-11. Detalles de integración de aplicaciones web de Okta



7 Configure el control de acceso de los usuarios.

En la sección **Assignments (Asignaciones) > Controlled access (Acceso controlado)**, tiene la opción de controlar si lo desea cuáles de los usuarios de Okta que existen en su organización pueden acceder a los clústeres de Tanzu Kubernetes Grid. En el ejemplo, permita que todos los definidos en la organización tengan acceso.

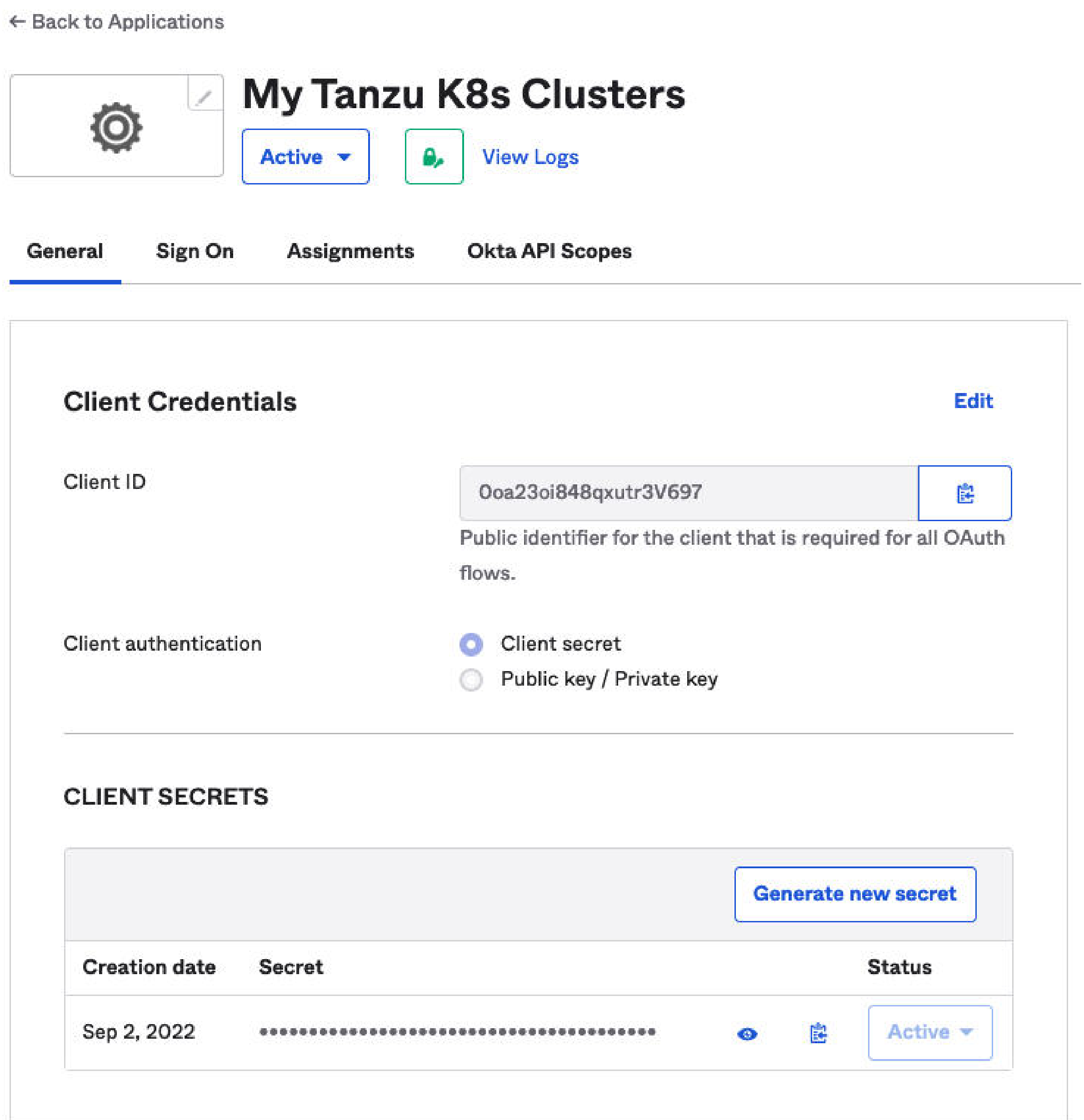
Figura 12-12. Control de acceso de Okta



8 Haga clic en **Save** (Guardar) y copie el **identificador de cliente** y el **secreto de cliente** que se devuelven.

Para guardar la configuración de Okta, la consola administrativa le proporciona un **ID de cliente** y un **secreto de cliente**. Copie ambos datos porque los va a necesitar para configurar Supervisor con un proveedor de identidad externo.

Figura 12-13. Identificador de cliente y secreto de OIDC

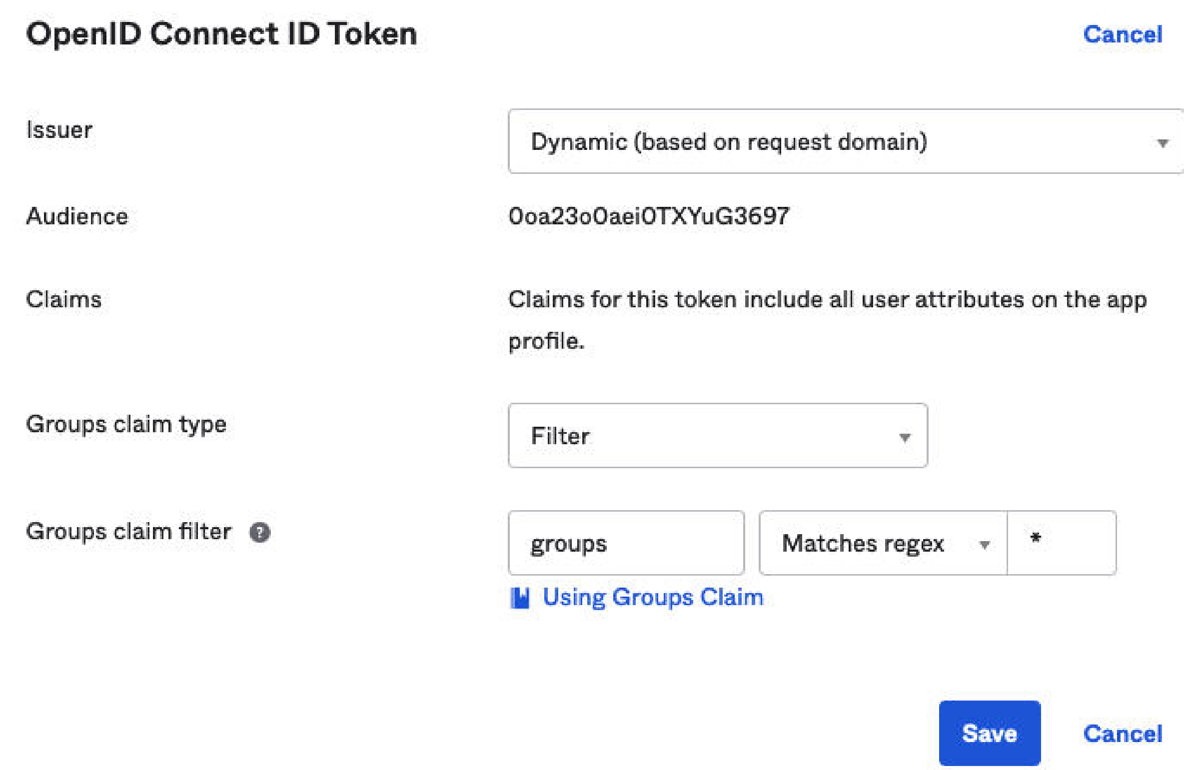


9 Configure el token de ID de OpenID Connect.

Haga clic en la pestaña **Sign On**. En la sección **OpenID Connect ID Token** (Token de ID de OpenID Connect), haga clic en el vínculo Edit (Editar), rellene el filtro **Groups claim type** (Tipo de notificación de grupos) y **guarde** la configuración.

Por ejemplo, si desea que el nombre de notificación "groups" coincida en todos los grupos, seleccione **groups > Matches regex >** *.

Figura 12-14. Token de ID de OpenID Connect

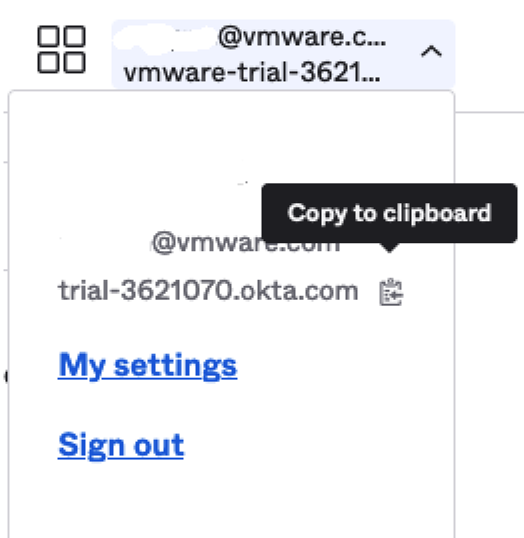


10 Copie la **URL del emisor**.

Para configurar el Supervisor, necesita la **URL del emisor**, además del **ID de cliente** y el **secreto de cliente**.

Copie la **URL del emisor** desde la consola administrativa de Okta.

Figura 12-15. URL del emisor de Okta



Registrar un IDP externo con Supervisor

Para conectarse a clústeres de Tanzu Kubernetes Grid 2.0 en Supervisor mediante la CLI de Tanzu, registre el proveedor de OIDC con Supervisor.

Requisitos previos

Antes de registrar un proveedor de ODIC externo con Supervisor, complete los siguientes requisitos previos:

- Habilite Administración de cargas de trabajo e implemente una instancia de Supervisor. Consulte Ejecutar clústeres de TKG 2.0 en Supervisor.
- Configure un proveedor de identidad externo OpenID Connect con la URL de devolución de llamada de Supervisor. Consulte Configurar un IDP externo para usarlo con clústeres de servicio TKG.
- Obtenga el identificador de cliente, el secreto de cliente y la URL del emisor del IDP externo. Consulte Configurar un IDP externo para usarlo con clústeres de servicio TKG.

Registrar un IDP externo con Supervisor

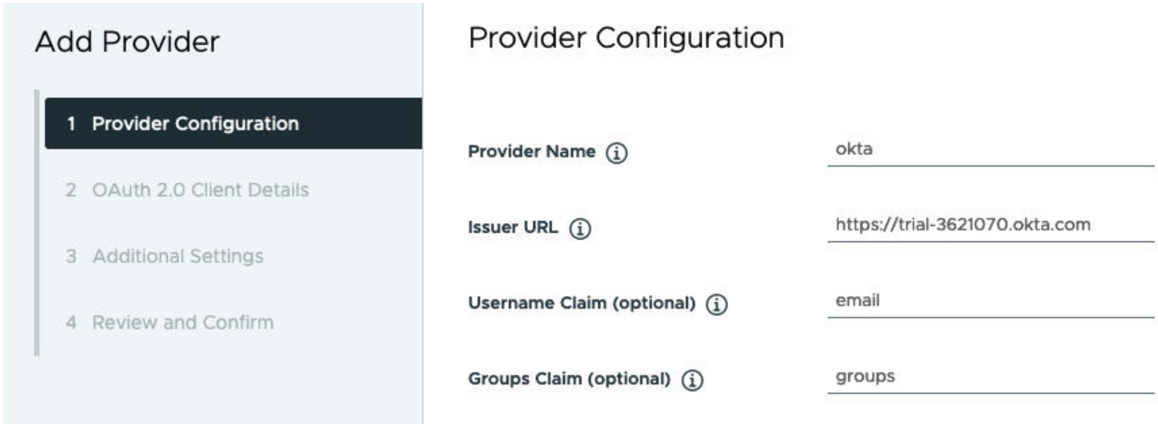
Supervisor ejecuta como pods los componentes Supervisor de Pinniped y Conserje de Pinniped. Los clústeres de Tanzu Kubernetes Grid solo ejecutan como pods el componente Conserje de Pinniped. Para obtener más información sobre estos componentes y cómo interactúan, consulte la documentación del servició de autenticación Pinniped.

Una vez que se registra un proveedor de identidad externo con Supervisor, el sistema actualiza los pods Supervisor y Conserje de Pinniped en Supervisor y los pods Conserje de Pinniped en clústeres de Tanzu Kubernetes Grid. Todos los clústeres de Tanzu Kubernetes Grid que se ejecutan en esa instancia de Supervisor se configuran automáticamente con ese mismo proveedor de identidad externo.

Para registrar un proveedor de ODIC externo con Supervisor, realice el siguiente procedimiento:

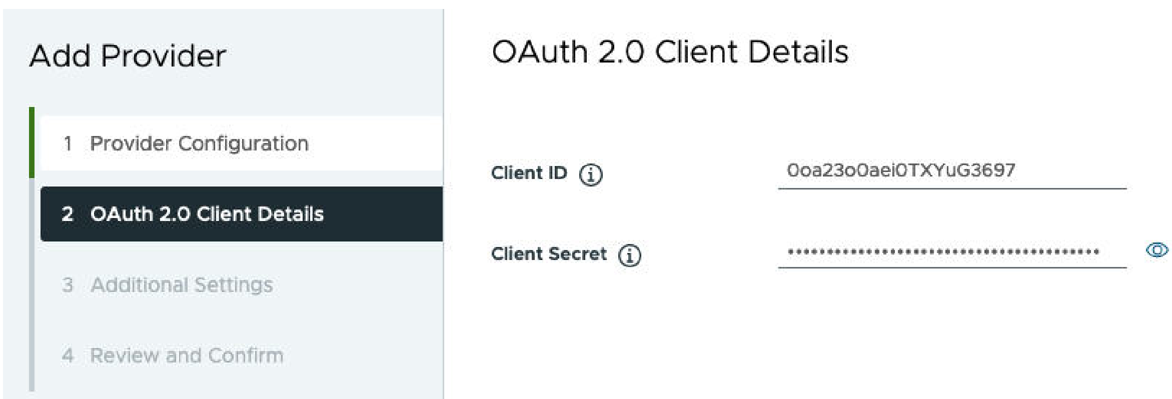
1. Inicie sesión en vCenter Server mediante vSphere Client.
2. Seleccione **Administración de cargas de trabajo > Supervisores > Configurar > Proveedores de identidad**.
3. Haga clic en el signo más para comenzar el proceso de registro.
4. Configure el proveedor. Consulte Configuración del proveedor de OIDC.

Figura 12-16. Configuración del proveedor de OIDC



5 Configure los detalles del cliente de OAuth 2.0. Consulte Detalles del cliente de OAuth 2.0.

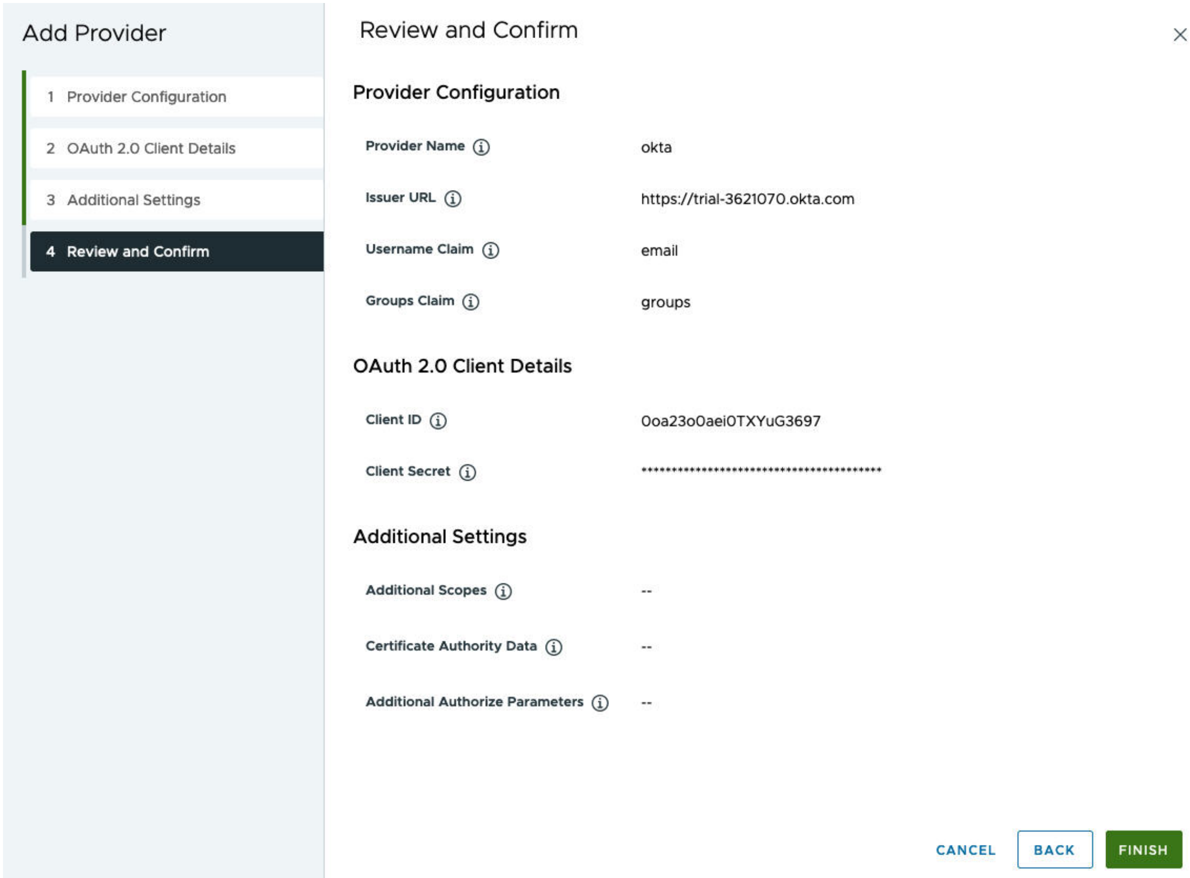
Figura 12-17. Detalles del cliente de OAuth 2.0



6 Configure los ajustes adicionales. Consulte Configuración adicional.

7 Confirme la configuración del proveedor.

Figura 12-18. Confirmar configuración del proveedor



8 Haga clic en **Finalizar** para completar el registro del proveedor de OIDC.

Configuración del proveedor de OIDC

Consulte los siguientes detalles de configuración del proveedor al registrar un proveedor de OIDC externo con Supervisor.

Tabla 12-1. Configuración del proveedor de OIDC

Campo	Importancia	Descripción
Nombre del proveedor	Obligatorio	El nombre definido por el usuario para el proveedor de identidad externo.
URL del emisor	Obligatorio	La URL del proveedor de identidad que emite tokens. La URL de detección de OIDC se deriva de la URL del emisor. Por ejemplo, para Okta, la URL del emisor puede ser similar a la siguiente y puede obtenerse en la consola de administración: *https://trial-4359939-admin.okta.com*.

Tabla 12-1. Configuración del proveedor de OIDC (continuación)

Campo	Importancia	Descripción
Notificación de nombre de usuario	Opcional	La notificación del token de identificador del proveedor de identidad ascendente o del endpoint de información de usuario que se va a inspeccionar para obtener el nombre de usuario para el usuario especificado. Si deja este campo vacío, la URL del emisor ascendente se concatena con la notificación "sub" para generar el nombre de usuario que se utilizará con Kubernetes. Este campo especifica lo que Pinniped debe examinar en el token de identificador ascendente para determinar la autenticación. Si no se proporciona, la identidad del usuario llevará el formato *https://IDP-ISSUER?sub=UUID*.
Notificación de grupos	Opcional	La notificación del token de identificador del proveedor de identidad ascendente o del endpoint de información de usuario que se va a inspeccionar para obtener los grupos para el usuario especificado. Si deja este campo vacío, no se utilizarán grupos del proveedor de identidad ascendente. El campo de notificaciones de grupos indica a Pinniped qué se debe buscar en el token de ID ascendente para autenticar la identidad del usuario.

Detalles del cliente de OAuth 2.0

Consulte los siguientes detalles del cliente OAuth 2.0 de proveedor al registrar un proveedor de OIDC externo con Supervisor.

Tabla 12-2. Detalles del cliente de OAuth 2.0

Detalles del cliente de OAuth 2.0	Importancia	Descripción
Identificador de cliente	Obligatorio	Identificador de cliente del IDP externo
Secreto del cliente	Obligatorio	Secreto de cliente del IDP externo

Configuración adicional

Consulte la siguiente configuración adicional al registrar un proveedor de OIDC externo con Supervisor.

Tabla 12-3. Configuración adicional

Configuración	Importancia	Descripción
Ámbitos adicionales	Opcional	Los ámbitos adicionales que se solicitarán en los tokens.
Datos de la entidad de certificación	Opcional	Datos de la entidad de certificación TLS para una conexión IDP externa segura
Parámetros de autorización adicionales	Opcional	Parámetros adicionales durante la solicitud de autorización de OAuth2

Cambiar la configuración de almacenamiento en el Supervisor

Las directivas de almacenamiento asignadas al Supervisor administran el modo en que se colocan los objetos como una máquina virtual de plano de control, el disco efímero de pod de vSphere y la memoria caché de imágenes de contenedor dentro de los almacenes de datos en el entorno de almacenamiento de vSphere. Por lo general, como administrador de vSphere debe configurar directivas de almacenamiento al habilitar el Supervisor. Si necesita realizar cambios en las asignaciones de directivas de almacenamiento después de la configuración inicial del Supervisor, realice esta tarea. También puede utilizar esta tarea para activar o desactivar la compatibilidad con volúmenes de archivos para volúmenes persistentes ReadWriteMany en clústeres de TKG.

Por lo general, los cambios que realice en la configuración de almacenamiento solo se aplican a los objetos nuevos de Supervisor. Si utiliza este procedimiento para activar la compatibilidad con volúmenes de archivos en clústeres de TKG, puede hacerlo para los clústeres existentes.

Requisitos previos

Si planea activar la compatibilidad con volúmenes de archivos en clústeres de TKG para volúmenes persistentes en modo ReadWriteMany, siga los requisitos previos de Crear volúmenes persistentes ReadWriteMany en vSphere IaaS control plane de la documentación de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

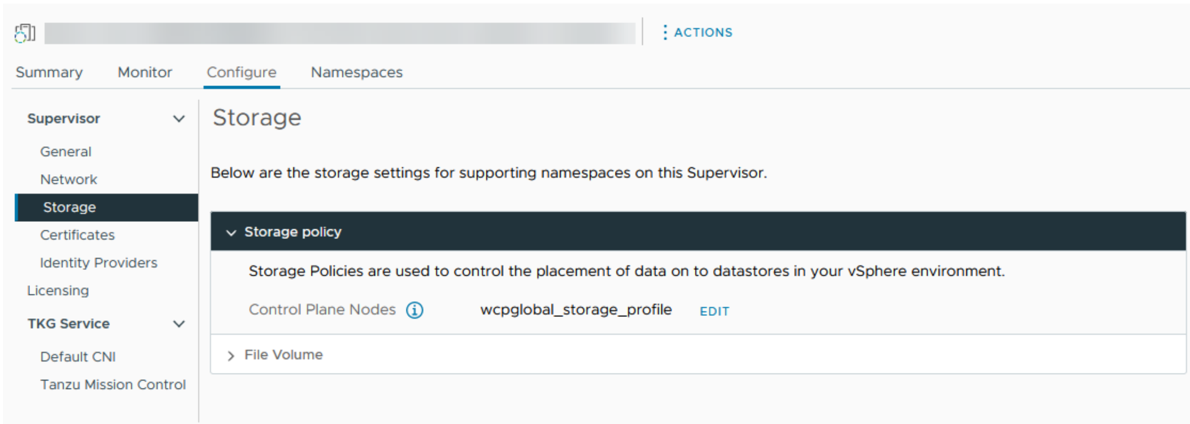
Procedimiento

1 En vSphere Client, desplácese hasta **Administración de cargas de trabajo**.

2 Haga clic en la pestaña **Supervisores** y seleccione el Supervisor que desea editar de la lista.

3 Haga clic en la pestaña **Configurar** y en **Almacenamiento**.

Figura 12-19. Actualización de la configuración de almacenamiento del supervisor



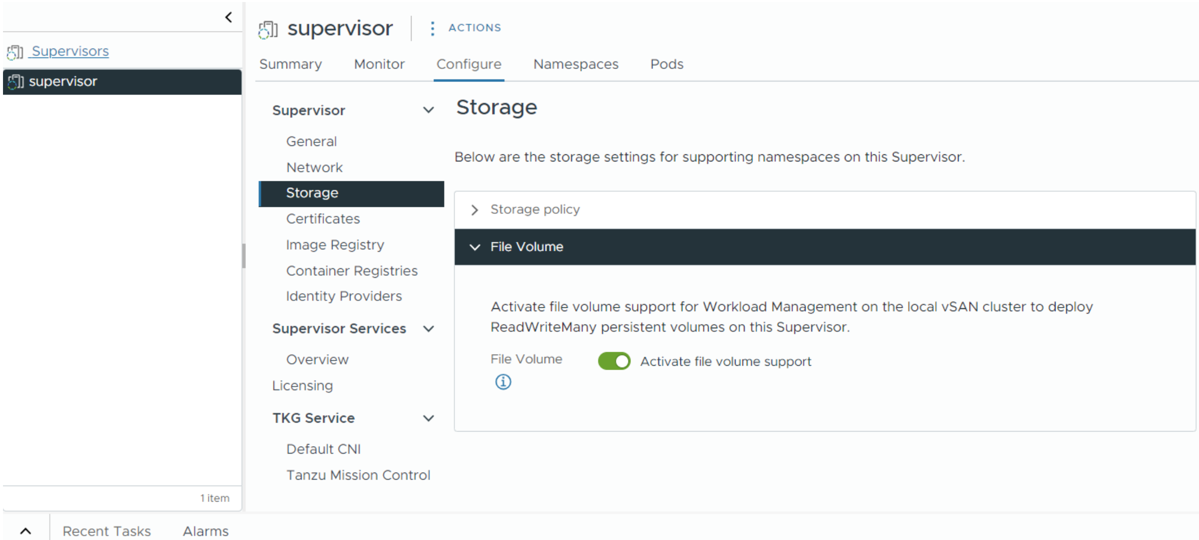
4 Cambie las asignaciones de directivas de almacenamiento para las máquinas virtuales del plano de control.

Si el entorno admite un pod de vSphere, también puede cambiar las directivas de almacenamiento para un disco virtual efímero y la memoria caché de imágenes de contenedor.

Opción	Descripción
Nodo del plano de control	Seleccione la directiva de almacenamiento para la colocación de las máquinas virtuales del plano de control.
Discos efímeros del pod	Seleccione la directiva de almacenamiento para la colocación de los pods de vSphere.
Memoria caché de imágenes de contenedor	Seleccione la directiva de almacenamiento para la colocación de la memoria caché de las imágenes de contenedor.

5 Habilite la compatibilidad con volúmenes de archivos para implementar volúmenes persistentes ReadWriteMany.

Esta opción solo está disponible si el entorno se configuró con el servicio de archivos de vSAN. Consulte Habilitar el servicio de archivos de vSAN.



Transmisión de métricas de Supervisor a una plataforma de observación personalizada

Aprenda a transmitir métricas de Supervisor recopiladas por Telegraf a una plataforma de observación personalizada. Telegraf se habilita de forma predeterminada en el Supervisor y recopila métricas en formato Prometheus de los componentes de Supervisor, como el servidor de API de Kubernetes, el servicio de máquina virtual y Tanzu Kubernetes Grid, entre otros. Como administrador de vSphere, puede configurar una plataforma de observación, como VMware Aria Operations for Applications, Grafana y otras, con la finalidad de ver y analizar las métricas de Supervisor recopiladas.

Telegraf es un agente basado en servidores que se utiliza para recopilar y enviar métricas procedentes de diferentes sistemas, bases de datos e IoT. Cada componente de Supervisor expone un endpoint al que se conecta Telegraf. Después, Telegraf envía las métricas recopiladas a la plataforma de observación que elija. Puede configurar alguno de los complementos de salida que Telegraf admite como plataforma de observación para agregar y analizar métricas de Supervisor. Consulte la documentación de Telegraf para obtener información sobre los complementos de salida compatibles.

Los siguientes componentes exponen endpoints a los que se conecta Telegraf y recopila métricas: servidor de API de Kubernetes, etcd, kubelet, administrador de controladores de Kubernetes, programador de Kubernetes, Tanzu Kubernetes Grid, servicio de máquina virtual, servicio de imagen de máquina virtual, NSX Container Plug-in (NCP), interfaz de almacenamiento de contenedor (Container Storage Interface, CSI), administrador de certificados, NSX y varias métricas de host, como CPU, memoria y almacenamiento.

Ver los pods y la configuración de Telegraf

Telegraf se ejecuta en el espacio de nombres del sistema `vmware-system-monitoring` en el Supervisor. Para ver los pods y ConfigMap de Telegraf:

1 Inicie sesión en el plano de control de Supervisor con una cuenta de administrador de vCenter Single Sign-On.

```
kubectl vsphere login --server <control plane IP> --vsphere-username
administrator@vsphere.local
```

2 Con el siguiente comando, vea los pods de Telegraf:

```
kubectl -n vmware-system-monitoring get pods
```

Los pods resultantes son los siguientes:

```
telegraf-csqsl
telegraf-dkwtk
telegraf-l4nxk
```

3 Con el siguiente comando, vea los ConfigMap de Telegraf:

```
kubectl -n vmware-system-monitoring get cm
```

Los ConfigMap resultantes son los siguientes:

```
default-telegraf-config
kube-rbac-proxy-config
kube-root-ca.crt
telegraf-config
```

El ConfigMap `default-telegraf-config` contiene la configuración predeterminada de Telegraf y es de solo lectura. Puede utilizarlo como opción de reserva para restaurar la configuración en `telegraf-config` en caso de que el archivo esté dañado o simplemente desee restaurar los valores predeterminados. El único ConfigMap que puede editar es `telegraf-config`, el cual define qué componentes envían métricas a los agentes de Telegraf y a qué plataformas.

4 Vea el ConfigMap de `telegraf-config`:

```
kubectl -n vmware-system-monitoring get cm telegraf-config -o yaml
```

La sección `inputs` del ConfigMap `telegraf-config` define todos los endpoints de los componentes de Supervisor en los que Telegraf recopila métricas, así como los tipos de métricas en sí. Por ejemplo, la siguiente entrada define el servidor de API de Kubernetes como un endpoint:

```
 [[inputs.prometheus]]
      # APIserver
      ## An array of urls to scrape metrics from.
      alias = "kube_apiserver_metrics"
      urls = ["https://127.0.0.1:6443/metrics"]
      bearer_token = "/run/secrets/kubernetes.io/serviceaccount/token"
      # Dropping metrics as a part of short term solution to vStats integration 1MB metrics
payload limit
      # Dropped Metrics:
      # apiserver_request_duration_seconds
      namepass = ["apiserver_request_total",
"apiserver_current_inflight_requests", "apiserver_current_inqueue_requests",
"etcd_object_counts", "apiserver_admission_webhook_admission_duration_seconds",
"etcd_request_duration_seconds"]
      # "apiserver_request_duration_seconds" has _massive_ cardinality, temporarily turned
off. If histogram, maybe filter the highest ones?
      # Similarly, maybe filters to _only_ allow error code related metrics through?
      ## Optional TLS Config
      tls_ca = "/run/secrets/kubernetes.io/serviceaccount/ca.crt"
```

La propiedad `alias` indica el componente desde el que se recopilan las métricas. La propiedad `namepass` especifica qué métricas de componentes exponen y recopilan respectivamente los agentes de Telegraf.

Aunque el ConfigMap `telegraf-config` ya contiene un amplio rango de métricas, puede definir otras adicionales. Consulte Métricas para componentes del sistema de Kubernetes y Referencia de métricas de Kubernetes.

Configurar la plataforma de observación en Telegraf

En la sección `outps` de `telegraf-config` puede configurar dónde transmite Telegraf las métricas que recopila. Existen varias opciones, como `outputs.file`, `outputs.wavefront`, `outputs.prometheus_client` y `outps-https`. La sección `outps-https` es donde puede configurar las plataformas de observación que desea utilizar para la adición y la supervisión de las métricas de Supervisor. Telegraf se puede configurar para enviar las métricas a más de una plataforma. Para editar el ConfigMap `telegraf-config` y configurar una plataforma de observación donde ver las métricas de Supervisor, siga los pasos que se indican a continuación:

1 Inicie sesión en el plano de control de Supervisor con una cuenta de administrador de vCenter Single Sign-On.

```
kubectl vsphere login --server <control plane IP> --vsphere-username
administrator@vsphere.local
```

2 Guarde el ConfigMap `telegraf-config` en la carpeta kubectl local:

```
kubectl get cm telegraf-config -n vmware-system-monitoring -o
jsonpath="{.data['telegraf\.conf']}">telegraf.conf
```

Asegúrese de almacenar el ConfigMap `telegraf-config` en un sistema de control de versiones antes de realizar cambios en él en caso de que desee restaurar una versión anterior del archivo. En caso de que desee restaurar la configuración predeterminada, puede utilizar los valores del ConfigMap `default-telegraf-config`.

3 Agregue secciones `outputs.http` con la configuración de conexión de las plataformas de observación que elija mediante un editor de texto, como VIM:

```
vim telegraf.config
```

Puede eliminar directamente la marca de comentario de la siguiente sección y editar los valores según corresponda, o bien puede agregar una sección `outputs.http` nueva según sea necesario.

```
    #[[outputs.http]]
    #   alias = "prometheus_http_output"
    #   url = "<PROMETHEUS_ENDPOINT>"
    #   insecure_skip_verify = <PROMETHEUS_SKIP_INSECURE_VERIFY>
    #   data_format = "prometheusremotewrite"
    #   username = "<PROMETHEUS_USERNAME>"
    #   password = "<PROMETHEUS_PASSWORD>"
    #   <DEFAULT_HEADERS>
```

Por ejemplo, así sería una configuración de `outputs.http` para Grafana:

```
    [[outputs.http]]
 url = "http://<grafana-host>:<grafana-metrics-port>/<prom-metrics-push-path>"
 data_format = "influx"
 [outputs.http.headers]
   Authorization = "Bearer <grafana-bearer-token>"
```

Consulte Transferir métricas desde Telegraf a Grafana para obtener más información sobre cómo configurar paneles de control y consumir métricas de Telegraf.

A continuación se muestra un ejemplo con VMware Aria Operations for Applications (anteriormente conocido como Wavefront):

```
    [[outputs.wavefront]]
      url = "http://<wavefront-proxy-host>:<wavefront-proxy-port>"
```

El método que se recomienda para introducir métricas en Aria Operations for Applications es a través de un proxy. Consulte Proxies de Wavefront para obtener más información.

4 Reemplace el archivo `telegraf-config` existente en el Supervisor por el que editó en su carpeta local:

```
kubectl create cm --from-file telegraf.conf -n vmware-system-monitoring telegraf-config
--dry-run=client -o yaml | kubectl replace -f -
```

5 Compruebe si la nueva configuración se ha guardado correctamente:

- Vea el nuevo ConfigMap `telegraf-config`:

  ```
  kubectl -n vmware-system-monitoring get cm telegraf-config -o yaml
  ```

- Compruebe si todos los pods de Telegraf están en funcionamiento:

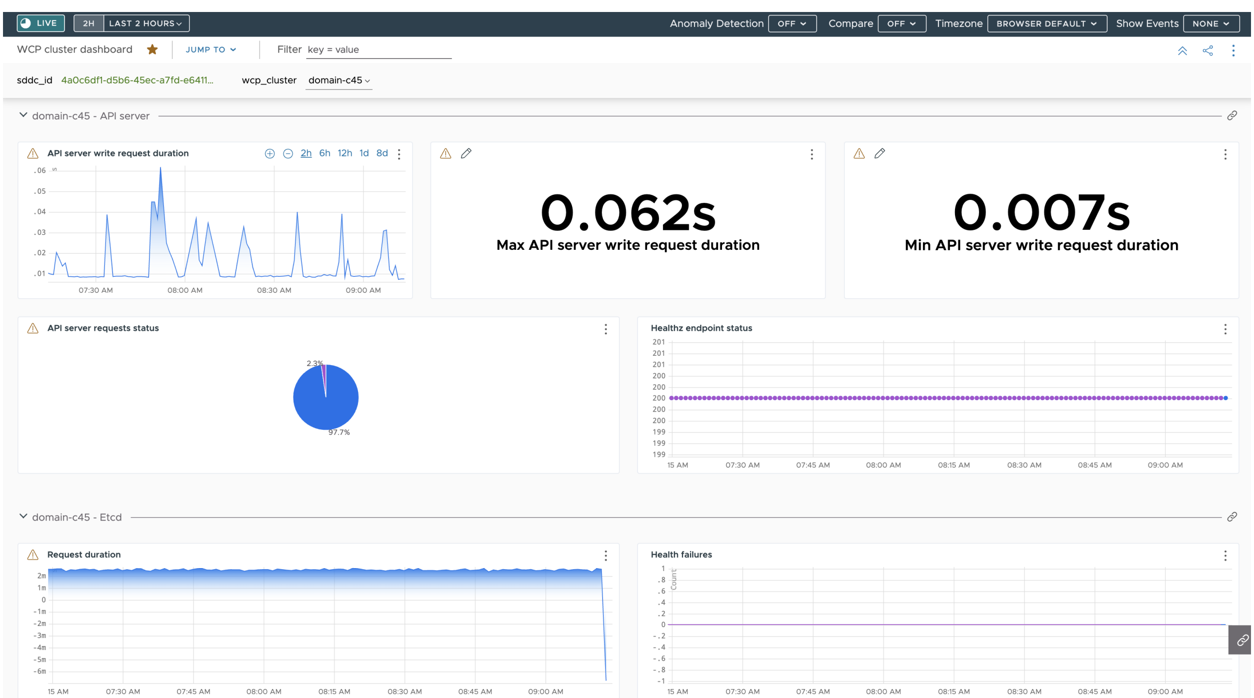
  ```
  kubectl -n vmware-system-monitoring get pods
  ```

- En caso de que algunos de los pods de Telegraf no se estén ejecutando, compruebe los registros de Telegraf para ese pod para solucionar los problemas:

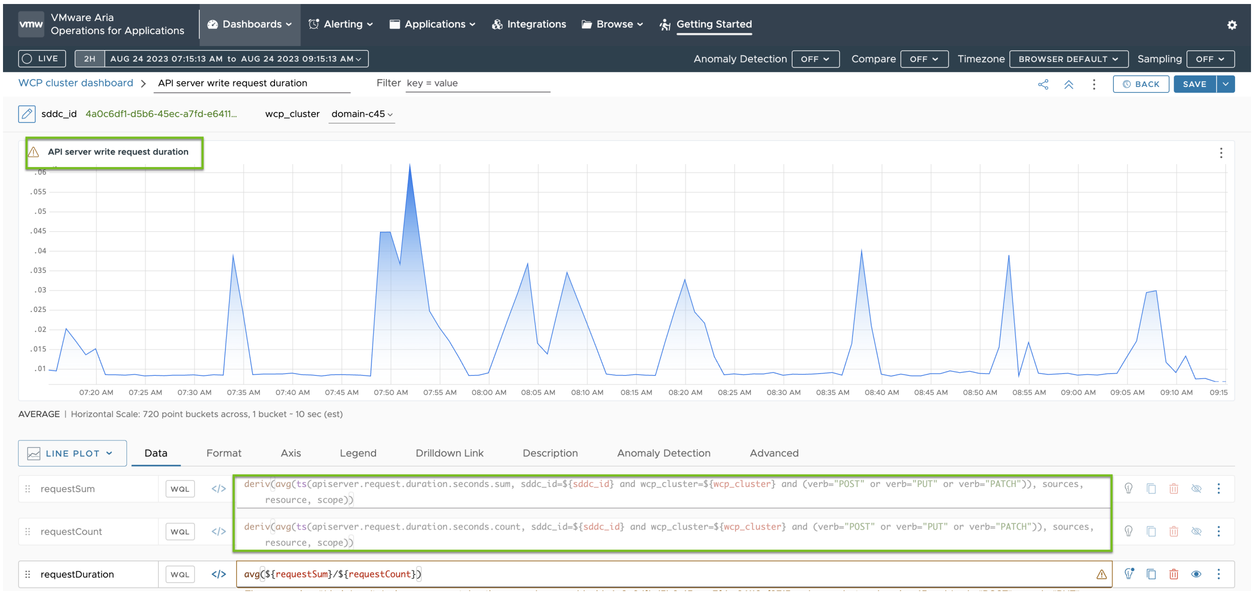
  ```
  kubectl -n vmware-system-monitoring logs <telegraf-pod>
  ```

Paneles de control de ejemplo de Operations for Applications

A continuación se muestra un panel de control con un resumen de las métricas recibidas desde el servidor de API y etcd en un Supervisor a través de Telegraf:



Las métricas para la duración de la solicitud de escritura del servidor de API se basan en las métricas que se especifican en el ConfigMap `telegraf-config` como se puede ver resaltado en verde:



Modificar la lista de nombres DNS del plano de control del Supervisor

Consulte cómo modificar la lista de los FQDN para acceder al plano de control de Supervisor. Puede proporcionar una lista de los FQDN de Supervisor durante la habilitación del Supervisor y actualizar esa lista más adelante. También puede definir una lista de los FQDN de Supervisor si no proporcionó una durante la habilitación de Supervisor.

Procedimiento

- Utilice el siguiente comando de la DCLI para actualizar la lista de los FQDN del plano de control del Supervisor:

  ```
  dcli com vmware vcenter namespacemanagement clusters update --cluster <cluster_ID> --
  master-dns-name <FQDN 1> --master-dns-name <FQDN_2>
  ```

  - Para agregar un nuevo FQDN a la lista, apruebe los nombres que ya están como argumentos y agregue el nuevo FQDN.
  - Para eliminar un FQDN de la lista, llame al comando `update` omitiendo el FQDN que desea quitar y aprobando el resto de los FQDN que desea conservar.

  Para un Supervisor de tres zonas, puede transferir el identificador de cualquiera de los clústeres que forman parte del Supervisor.

  En el siguiente ejemplo, el Supervisor que se ejecuta en el clúster `domain-c50` ya está configurado con un FQDN `supervisor.acme.com`. Va a agregar un FQDN de `supervisor.vmware.com` nuevo a la lista de nombres DNS del Supervisor:

  ```
  dcli com vmware vcenter namespacemanagement clusters update --cluster domain-c50 --master-
  dns-name supervisor.acme.com --master-dns-name supervisor.vmware.com
  ```

Pasos siguientes

- El certificado VIP para conectarse de forma segura al Supervisor no se actualiza automáticamente con los nuevos FQDN. Por lo tanto, debe hacerlo manualmente; consulte Reemplazar el certificado VIP para conectarse de forma segura al endpoint de API de Supervisor.
- Una vez que actualice el certificado VIP para conectarse al Supervisor, inicie sesión en el plano de control de Supervisor mediante los FQDN recién agregados. Consulte Conectarse al Supervisor como usuario vCenter Single Sign-On.

Reenviar registros de Supervisor a sistemas de supervisión externos

Consulte cómo configurar el reenvío de registros del plano de control de Supervisor a sistemas de supervisión externos, como Grafana Loki o Elastic Search, mediante Fluent Bit.

Los registros del plano de control de Supervisor se reenvían automáticamente al servidor syslog configurado en el dispositivo vCenter Server mediante Fluent Bit. Fluent Bit es un reenviador y procesador de métricas y registros ligero de código abierto que proporciona configuraciones para admitir varios tipos de datos de registro, filtros y mejoras de etiquetas de registro.

Durante la activación o la actualización de Supervisor, rsyslog sigue reenviando los registros de arranque a los servidores syslog que están configurados en el dispositivo vCenter Server. Una vez que las máquinas virtuales del plano de control de Supervisor están en funcionamiento, Fluent Bit se convierte en el reenviador de registros predeterminado para los registros del plano de control de Supervisor.

Como administrador de vSphere, puede utilizar Fluent Bit para lo siguiente:

- Reenviar registros del plano de control y registros del sistema de Supervisor a las principales plataformas externas de supervisión de registros, como Loki, Elastic Search, Grafana y otras plataformas compatibles con Fluent Bit.
- Actualizar o restablecer la configuración de reenvío de registros para el plano de control de Supervisor mediante la API de k8s.

Fluent Bit se ejecuta como un DeamonSet en los nodos del plano de control de Supervisor. Expone el ConfigMap `fluentbit-config-custom` en el espacio de nombres `vmware-system-logging` que los administradores de vSphere pueden editar para configurar el reenvío de registros a plataformas externas mediante la definición de servidores de registro.

```
inputs-custom.conf: |
  [INPUT]
      Name              tail
      Alias             audit_apiserver_tail
      Tag               audit.apiserver.*
      Path              /var/log/vmware/audit/kube-apiserver.log
      DB                /var/log/vmware/fluentbit/flb_audit_apiserver.db
      Buffer_Max_Size   12MBb
```

```
      Mem_Buf_Limit     32MB
      Skip_Long_Lines   On
      Refresh_Interval  10

filters-custom.conf: |
  [FILTER]
      Name           record_modifier
      Alias          audit_apiserver_modifier
      Match          audit.apiserver.*
      Record         hostname ${NODE_NAME}
      Record         appname audit-kube-apiserver
      Record         filename kube-apiserver.log

outputs-custom.conf: |
  [OUTPUT]
     Name                 syslog
     Alias                audit_apiserver_output_syslog
     Match                audit.apiserver.*
     Host                 <syslog-server-host>
     Port                 <syslog-server-port>
     Mode                 tcp
     Syslog_Format        rfc5424
     Syslog_Message_key   log
     Syslog_Hostname_key  hostname
     Syslog_Appname_key   appname
     Syslog_Msgid_key     filename
```

Personalizar el reenvío de registros de Fluent Bit

Siga los pasos para personalizar la configuración de reenvío de registros de Fluent Bit:

1 Inicie sesión en el plano de control de Supervisor como administrador de vCenter Single Sign-On.

```
> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

2 Actualice o agregue una salida de syslog en la sección `outputs-custom.conf` de ConfigMap `fluentbit-config-custom`, que reenviará todos los registros del sistema de la máquina virtual del plano de control a un servidor externo.

```
[OUTPUT]
     Name                 syslog
     Alias                syslog_system
     Match                system*
     Host                 <syslog-server-host>
     Port                 <syslog-server-port>
     Mode                 tcp
     Syslog_Format        rfc5424
     Syslog_Message_key   log
     Syslog_Hostname_key  hostname
     Syslog_Appname_key   appname
```

```
     Syslog_Msgid_key     filename
     # add the following if the mode is TLS
     Tls                  on
     Tls.verify           off
     Tls.ca_file          /etc/ssl/certs/vmca.pem
```

3 Aplique los cambios al ConfigMap `fluentbit-config-custom`.

```
> kubectl -n vmware-system-logging edit cm fluentbit-config-custom

# use the below command if the change is stored in outputs-custom.conf file
> kubectl -n vmware-system-logging create configmap fluentbit-config-custom --from-
file=filters-custom.conf --from-file=inputs-custom.conf --from-file=outputs-custom.conf -o
yaml --from-file=parsers-custom.conf --dry-run | kubectl replace -f -
```

4 Supervise el pod de Fluent Bit para aplicar automáticamente los cambios de configuración y consulte los registros de Supervisor en el servidor syslog. Si el DaemonSet de Fluentbit se ejecuta con un error después de actualizar la configuración, repare o restablezca la configuración en el ConfigMap `fluentbit-config-custom` para asegurarse de que el DaemonSet de Fluentbit esté en buen estado.

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Reenviar registros de auditoría del servidor de API de Kubernetes a un servidor Grafana Loki

Siga los pasos para configurar el reenvío de registros a un servidor Grafana Loki externo:

1 Inicie sesión en el plano de control de Supervisor como administrador de vCenter Single Sign-On.

```
> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

2 Actualice o agregue un resultado de Loki en la sección `outputs-custom.conf` del ConfigMap `fluentbit-config-custom`, que reenviará todos los registros del sistema de la máquina virtual del plano de control al servidor de registros de Loki.

```
[OUTPUT]
        Name loki
        Alias system_output_loki
        Match system*
        Host <loki-server-host>
        Port <loki-server-port>
        Labels $hostname,$appname,$filename,$procid,$labels
```

3 Aplique los cambios al ConfigMap `fluentbit-config-custom`.

```
> kubectl -n vmware-system-logging edit cm fluentbit-config-custom

# use the below command if the change is stored in outputs-custom.conf file
> kubectl -n vmware-system-logging create configmap fluentbit-config-custom --from-
file=filters-custom.conf --from-file=inputs-custom.conf --from-file=outputs-custom.conf -o
yaml --from-file=parsers-custom.conf --dry-run | kubectl replace -f -
```

4 Supervise el pod de Fluent Bit para aplicar automáticamente los cambios de configuración y consulte los registros de Supervisor en el servidor syslog. Si el DaemonSet de Fluentbit se ejecuta con un error después de actualizar la configuración, repare o restablezca la configuración en el ConfigMap `fluentbit-config-custom` para asegurarse de que el DaemonSet de Fluentbit esté en buen estado.

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Reenviar registros a Elastic Search

Siga los pasos para configurar el reenvío de registros a un servidor de Elastic Search externo:

1 Inicie sesión en el plano de control de Supervisor como administrador de vCenter Single Sign-On.

```

> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

2 Actualice o agregue un resultado de Elastic Search en la sección `outputs-custom.conf` del ConfigMap `fluentbit-config-custom`, que reenviará todos los registros del sistema de la máquina virtual del plano de control al servidor de registro ES.

```
[OUTPUT]
       Name es
       Alias system_output_es
       Match system*
       Host <es-server-host>
       Port <es-server-port>
       Index supervisor
       Type controlplanevm
```

3 Aplique los cambios al ConfigMap `fluentbit-config-custom`.

```
> kubectl -n vmware-system-logging edit cm fluentbit-config-custom

# use the below command if the change is stored in outputs-custom.conf file
> kubectl -n vmware-system-logging create configmap fluentbit-config-custom --from-
file=filters-custom.conf --from-file=inputs-custom.conf --from-file=outputs-custom.conf -o
yaml --from-file=parsers-custom.conf --dry-run | kubectl replace -f -
```

4

5 Supervise el pod de Fluent Bit para aplicar automáticamente los cambios de configuración y consulte los registros de Supervisor en el servidor syslog.

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Reenviar registros de auditoría de la API de Kubernetes a un servidor syslog

Siga los pasos para configurar el reenvío de registros de auditoría de la API de Kubernetes a un servidor syslog externo:

1 Agregue `kubectl-plugin-vsphere` y `authproxy` en el ConfigMap `fluentbit-config`:

```
[INPUT]
    Name              tail
    Tag               auth.kubectl-plugin.*
    Path              /var/log/containers/audit/kubectl-plugin-vsphere*.log
    DB                /var/log/vmware/fluentbit/flb_auth_kubectl-plugin.db
    Skip_Long_Lines   Off
    Refresh_Interval  10

[INPUT]
    Name              tail
    Tag               auth.authproxy.*
    Path              /var/log/containers/audit/wcp-authproxy*.log
    DB                /var/log/vmware/fluentbit/flb_auth_authproxy.db
    Skip_Long_Lines   Off
    Refresh_Interval  10
```

2 Agregue el filtro `kubectl-plugin-vsphere` y `authproxy` al ConfigMap `fluentbit-config`:

```
[FILTER]
    Name           kubernetes
    Match          auth.*
    Kube_URL       https://localhost:6443
    Tls.verify     Off
    K8S-Logging.Parser On
    K8S-Logging.Exclude On

[FILTER]
    Name           record_modifier
    Match          auth.*
    Operation      lift
    Nested_under   kubernetes

[FILTER]
    Name           modify
```

```
    Match          auth.*
    Rename         container_name appname
    Rename         host hostname
    Rename         pod_name procid
```

3 Agregue los resultados de `kubectl-plugin-vsphere` al servidor syslog al ConfigMap `fluentbit-config`:

```
[OUTPUT]
    Name                 syslog
    Match                auth.*
    Host                 <syslog-server-host>
    Port                 <syslog-server-port>
    Mode                 tcp
    Syslog_Format        rfc5424
    Syslog_Message_key   log
    Syslog_Hostname_key  hostname
    Syslog_Appname_key   appname
    Syslog_Msgid_key     filename
```

4 Incluya los archivos anteriores en el ConfigMap `fluentbit-config`, en el espacio de nombres `vmware-system-logging`.

```
> k -n vmware-system-logging edit cm fluentbit-config
> k -n vmware-system-logging rollout restart ds fluentbit
> k -n vmware-system-logging rollout status ds fluentbit
```

Implementar un Supervisor mediante la clonación de una configuración existente

13

Aprenda a implementar un Supervisor mediante la clonación de la configuración de un Supervisor existente. Clone un Supervisor si desea implementar una nueva instancia de Supervisor que tenga la misma configuración que un Supervisor que ya esté implementado.

Requisitos previos

- Complete los requisitos previos para configurar clústeres de vSphere como un Supervisor. Consulte Requisitos previos para configurar vSphere IaaS control plane en clústeres de vSphere.
- Implemente un Supervisor.

Procedimiento

1 Vaya a **Administración de cargas de trabajo > Supervisor > Supervisores**.

2 Seleccione el Supervisor que desee clonar y seleccione **Clonar configuración**.

   Se abrirá el asistente de activación de Supervisor con los valores rellenados previamente en el Supervisor que seleccionó.

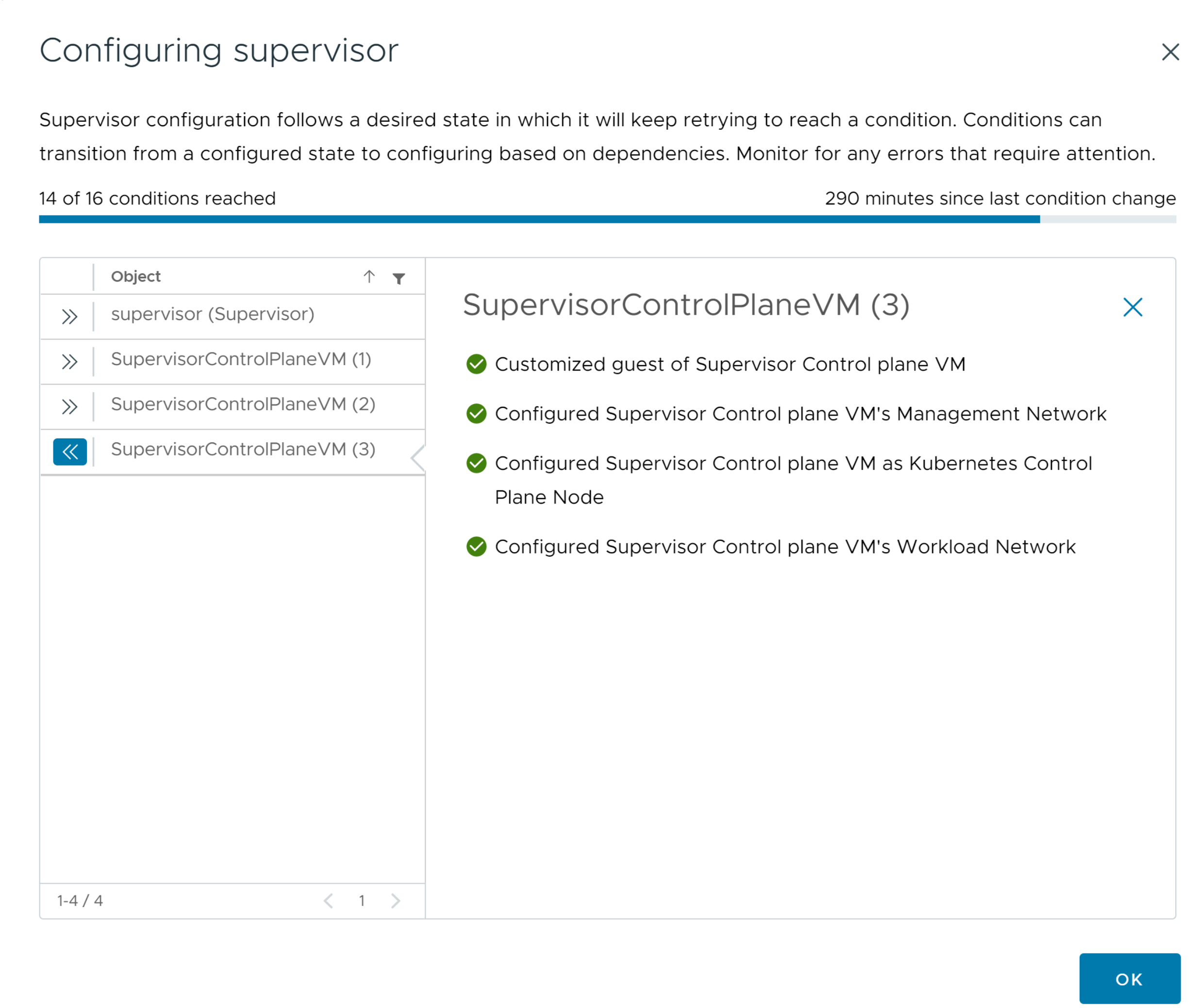
3 Revise el asistente modificando los valores según sea necesario.

   Para obtener más información sobre los valores del asistente, consulte Capítulo 5 Implementar Supervisor de tres zonas y Capítulo 6 Implementar un Supervisor de una sola zona .

Pasos siguientes

Una vez completado el asistente para habilitar Supervisor, podrá realizar un seguimiento del proceso de activación y observar los posibles problemas que se deban solucionar. En la columna **Estado de configuración**, haga clic en **Ver** junto al estado del Supervisor.

Figura 13-1. Vista de activación del supervisor



Para que se complete el proceso de implementación, el Supervisor debe alcanzar el estado deseado, lo que significa que se cumplen las 16 condiciones. Cuando un Supervisor se habilita correctamente, su estado cambia de Configurando a En ejecución. Mientras el Supervisor se encuentra en el estado Configurando, se vuelve a intentar de forma continua alcanzar cada una de las 16 condiciones. Si no se alcanza una condición, se vuelve a intentar la operación hasta que se completa correctamente. Por este motivo, el número de condiciones que se alcanzan puede cambiar una y otra vez, por ejemplo, *10 de 16 condiciones alcanzadas*, luego *4 de 16 condiciones alcanzadas* y así sucesivamente. En casos excepcionales, el estado puede cambiar a Error si existen errores que impiden alcanzar el estado deseado.

Para obtener más información sobre los errores de implementación y la forma de solucionarlos, consulte Resolver los estados de errores en las máquinas virtuales del plano de control de un Supervisor durante una activación o una actualización.

Solucionar problemas de habilitación de Supervisor

14

Descubra cómo solucionar los problemas de habilitación de Supervisor para que se alcance el estado deseado y se cumplan las 16 condiciones de habilitación.

Lea los siguientes temas a continuación:

Resolver los estados de errores en las máquinas virtuales del plano de control de un Supervisor durante una activación o una actualización

Después de activar un Supervisor, actualizar la versión de Supervisor Kubernetes o editar la configuración de un Supervisor existente, toda la configuración que haya especificado se validará y se aplicará al Supervisor hasta que se complete la configuración. Las comprobaciones de estado se realizan en los parámetros introducidos que pueden detectar errores en la configuración, lo que da como resultado un estado de error de Supervisor. Debe resolver estos estados de error para que sea posible la configuración o la actualización del Supervisor.

Tabla 14-1. Errores de conexión de vCenter Server

Mensaje de error	Motivo	Solución
No se puede resolver el identificador de red principal de vCenter <*FQDN*> con los servidores DNS de administración configurados en la máquina virtual del plano de control <*nombre de la máquina virtual*>. Valide que los servidores DNS de administración <nombre del servidor> puedan resolver <*nombre de la red*>.	■ Se puede acceder al menos a un servidor DNS de administración. ■ Se proporciona al menos un DNS de administración de forma estática. ■ Los servidores DNS de administración no tienen ninguna búsqueda de nombre de host para el PNID de vCenter Server. ■ El PNID de vCenter Server es un nombre de dominio, no una dirección IP estática.	■ Agregue una entrada de host para el PNID de vCenter Server a los servidores DNS de administración. ■ Compruebe que los servidores DNS configurados sean correctos.
No se puede resolver el identificador de red principal de vCenter <*nombre de la red*> con los servidores DNS adquiridos a través de DHCP en la red de administración de la máquina virtual del plano de control <*nombre de la máquina virtual*>. Valide que los servidores DNS de administración puedan resolver <*nombre de la red*>.	■ Se puede acceder a los servidores DNS de administración suministrados por el servidor DHCP (al menos uno). ■ Los servidores DNS de administración se suministran de forma estática. ■ Los servidores DNS de administración no tienen ninguna búsqueda de nombre de host para el PNID de vCenter Server. ■ Los servidores DNS de administración no tienen ninguna búsqueda de nombre de host para el PNID de vCenter Server. ■ El PNID de vCenter Server es un nombre de dominio, no una dirección IP estática.	■ Agregue una entrada de host para el PNID de vCenter Server a los servidores DNS de administración suministrados por el servidor DHCP configurado. ■ Compruebe que los servidores DNS que proporciona el servidor DHCP sean correctos.
No se puede resolver el host<*nombre del host*> en la máquina virtual del plano de control <*nombre de la máquina virtual*, ya que no hay servidores DNS de administración configurados.	■ El PNID de vCenter Server es un nombre de dominio, no una dirección IP estática. ■ No hay servidores DNS configurados.	Configure un servidor DNS de administración.
No se puede resolver el host <*nombre del host*> en la máquina virtual del plano de control <*nombre de la máquina virtual*>. El nombre de host termina con el dominio de nivel superior '.local', que requiere que se incluya 'local' en los dominios de búsqueda de DNS de administración.	El PNID de vCenter Server contiene `.local` como dominio de nivel superior (top-level domain, TLD), pero los dominios de búsqueda configurados no incluyen `local`.	Agregue `local` a los dominios de búsqueda de DNS de administración.

Tabla 14-1. Errores de conexión de vCenter Server (continuación)

Mensaje de error	Motivo	Solución
No se puede conectar a los servidores DNS de administración <*nombre del servidor*> desde la máquina virtual del plano de control <*nombre de la máquina virtual*>. Se intentó la conexión a través de la red de carga de trabajo.	■ Los servidores DNS de administración no se pueden conectar a vCenter Server. ■ Los valores de `worker_dns` proporcionados contienen en su totalidad los valores de DNS de administración proporcionados. Esto significa que el tráfico se enruta a través de la red de carga de trabajo, ya que Supervisor debe elegir una interfaz de red para dirigir el tráfico estático a estas direcciones IP.	■ Compruebe la red de carga de trabajo para verificar que se puede enrutar a los servidores DNS de administración configurados. ■ Compruebe que no haya direcciones IP en conflicto que puedan activar el enrutamiento alternativo entre los servidores DNS y otros servidores de la red de carga de trabajo. ■ Compruebe que el servidor DNS configurado sea, de hecho, un servidor DNS y que aloje su puerto DNS en el puerto 53. ■ Compruebe que los servidores DNS de carga de trabajo estén configurados para permitir conexiones desde las direcciones IP de las máquinas virtuales del plano de control (las direcciones IP proporcionadas por la red de carga de trabajo). ■ Compruebe que no haya errores ortográficos en las direcciones de los servidores DNS de administración. ■ Compruebe que los dominios de búsqueda no incluyan un '~' innecesario que podría estar resolviendo el nombre de host de forma incorrecta.

Tabla 14-1. Errores de conexión de vCenter Server (continuación)

Mensaje de error	Motivo	Solución
No se puede conectar a los servidores DNS de administración <*nombre del servidor*> desde la máquina virtual del plano de control <*nombre de la máquina virtual*>.	No se puede conectar a los servidores DNS.	■ Revise la red de administración para comprobar que existen rutas a los servidores DNS de administración. ■ Compruebe que no haya direcciones IP en conflicto que puedan activar el enrutamiento alternativo entre los servidores DNS y otros servidores. ■ Compruebe que el servidor DNS configurado sea, de hecho, un servidor DNS y que aloje su puerto DNS en el puerto 53. ■ Compruebe que los servidores DNS de administración estén configurados para permitir conexiones desde las direcciones IP de las máquinas virtuales del plano de control. ■ Compruebe que no haya errores ortográficos en las direcciones de los servidores DNS de administración. ■ Compruebe que los dominios de búsqueda no incluyan un '~' innecesario que podría estar resolviendo el nombre de host de forma incorrecta.
No se puede conectar a <*nombre del componente*> <*dirección del componente*> desde la máquina virtual del plano de control <nombre de la máquina virtual>. Error: *texto del mensaje de error*	■ Se produjo un error de red genérico. ■ Se produjo un error al conectarse a la conexión real a vCenter Server.	■ Valide que el nombre de host o la dirección IP de los componentes configurados, como vCenter Server, HAProxy, NSX Manager o NSX Advanced Load Balancer, sean correctos. ■ Valide cualquier configuración de red externa, como direcciones IP en conflicto, reglas de firewall y otras, en la red de administración.

Tabla 14-1. Errores de conexión de vCenter Server (continuación)

Mensaje de error	**Motivo**	**Solución**
La máquina virtual del plano de control <*nombre de la máquina virtual*> no pudo validar el certificado de vCenter <*nombre de vCenter Server*>. El certificado de vCenter Server no es válido.	El certificado proporcionado por vCenter Server tiene un formato no válido y, por lo tanto, no es de confianza.	■ Reinicie `wcpsvc` para comprobar que el paquete de raíces de confianza en las máquinas virtuales del plano de control esté actualizado con los certificados raíz de vCenter Server más recientes. ■ Compruebe que el certificado de vCenter Server sea válido.
La máquina virtual del plano de control <*nombre de la máquina virtual*> no confía en el certificado de vCenter <*nombre de vCenter Server*>.	■ El certificado `vmca.pem` que presenta vCenter Server es diferente de lo que está configurado para las máquinas virtuales del plano de control. ■ Los certificados raíz de confianza se reemplazaron en el dispositivo de vCenter Server, pero `wcpsvc` no se reinició.	■ Reinicie `wcpsvc` para comprobar que el paquete de raíces de confianza en las máquinas virtuales del plano de control esté actualizado con las raíces de certificado de vCenter Server más recientes.

Tabla 14-2. Errores de conexión de NSX Manager

La máquina virtual del plano de control <*nombre de la máquina virtual*> no pudo validar el certificado del servidor NSX <*nombre del servidor NSX*>. La huella digital que devuelve el servidor <*dirección de NSX-T*> no coincide con la huella digital de certificado del cliente esperada registrada en vCenter <*nombre de vCenter Server*>	Las huellas digitales SSL registradas en el Supervisor no coinciden con el hash SHA-1 del certificado que presenta NSX Manager.	■ Vuelva a habilitar la confianza en NSX Manager entre NSX y la instancia de vCenter Server. ■ Reinicie `wcpsvc` en vCenter Server.
No se puede conectar a <*nombre del componente*> <*dirección del componente*> desde la máquina virtual del plano de control <*nombre de la máquina virtual*>. Error: *texto del mensaje de error*	Se produjo un error de red genérico.	■ Valide cualquier configuración de red externa, direcciones IP en conflicto, reglas de firewall y otros elementos en la red de administración para NSX Manager. ■ Compruebe que la dirección IP de NSX Manager en la extensión de NSX sea correcta. ■ Compruebe que NSX Manager se esté ejecutando.

Tabla 14-3. Errores del equilibrador de carga

La máquina virtual del plano de control <*nombre de máquina virtual*> no confía en el certificado del equilibrador de carga (<*equilibrador de carga*> - <*endpoint del equilibrador de carga*>).	El certificado que presenta el equilibrador de carga es diferente del certificado que está configurado para las máquinas virtuales del plano de control.	Compruebe que haya configurado el certificado TLS de administración correcto para el equilibrador de carga.
La máquina virtual del plano de control <*nombre de máquina virtual*> no pudo validar el certificado del equilibrador de carga (<*equilibrador de carga*> - <*endpoint del equilibrador de carga*>. El certificado no es válido.	El certificado que presenta el equilibrador de carga tiene un formato no válido o ha caducado.	Corrija el certificado del servidor del equilibrador de carga configurado.
La máquina virtual del plano de control <*nombre de la máquina virtual*> no pudo autenticarse en el equilibrador de carga (<*equilibrador de carga*> - <*endpoint del equilibrador de carga*> con el nombre de usuario <*nombre de usuario*> y la contraseña proporcionada.	El nombre de usuario o la contraseña del equilibrador de carga son incorrectos.	Compruebe si el nombre de usuario y la contraseña configurados en el equilibrador de carga son correctos.
Se produjo un error de HTTP al intentar conectarse al equilibrador de carga (<*equilibrador de carga*> - <*endpoint del equilibrador del carga*> desde la máquina virtual del plano de control <*nombre de la máquina virtual*>).	Las máquinas virtuales del plano de control pueden conectarse al endpoint del equilibrador de carga, pero el endpoint no devuelve una respuesta http correcta (200).	Compruebe que el equilibrador de carga esté en buen estado y acepte solicitudes.
No se puede conectar al <*equilibrador de carga*> (<*endpoint del equilibrador de carga*>) desde la máquina virtual del plano de control <*nombre de la máquina virtual*>. Error: <*texto de error*>	■ Se produjo un error de red genérico. ■ Por lo general, significa que el equilibrador de carga no funciona o que algún firewall bloquea la conexión.	■ Validar que se puede acceder al endpoint del equilibrador de carga ■ Valide que no haya firewalls que bloqueen la conexión con el equilibrador de carga.

Transmitir registros del plano de control de Supervisor a un rsyslog remoto

Compruebe cómo configurar la transmisión de registros desde las máquinas virtuales del plano de control de Supervisor hacia un receptor rsyslog remoto para evitar la pérdida de datos de registro valiosos.

Los registros generados por los componentes en las máquinas virtuales del plano de control de Supervisor se almacenan localmente en los sistemas de archivos de las máquinas virtuales. Cuando se acumula una gran cantidad de registros, los registros se rotan a alta velocidad, lo que provoca la pérdida de mensajes valiosos que pueden ayudar a identificar la causa principal de diferentes problemas. vCenter Server y las máquinas virtuales del plano de control de Supervisor admiten la transmisión de sus registros locales a un receptor rsyslog remoto. Esta función ayuda a capturar registros para los siguientes servicios y componentes:

- En vCenter Server: servicio del plano de control de carga de trabajo, servicio de ESX Agent Manager, servicio de entidad de certificación y todos los demás servicios que se ejecutan en vCenter Server.
- Componentes del plano de control de Supervisor y servicios integrados de Supervisor, como el servicio de máquina virtual, y Tanzu Kubernetes Grid.

Puede configurar el dispositivo de vCenter Server para recopilar y transmitir datos de registro locales a un receptor rsyslog remoto. Una vez que esta configuración se aplica a vCenter Server, el remitente de rsyslog que se ejecuta dentro de vCenter Server comienza a enviar registros generados por los servicios dentro de ese sistema vCenter Server.

Supervisor utiliza el mismo mecanismo que vCenter Server para descargar registros locales con el fin de reducir la sobrecarga de administración de la configuración. El servicio del plano de control de carga de trabajo supervisa la configuración de rsyslog de vCenter Server mediante registros de sondeo periódicamente. Si el servicio del plano de control de carga de trabajo detecta que la configuración de rsyslog del vCenter Server remoto no está vacía, el servicio propaga esta configuración a cada máquina virtual del plano de control en todos los Supervisores. Esto puede generar una gran cantidad de tráfico de mensajes rsyslog que puede sobrecargar al receptor rsyslog remoto. Por lo tanto, la máquina receptora debe tener suficiente capacidad de almacenamiento para soportar grandes cantidades de mensajes rsyslog.

Al eliminar la configuración de rsyslog de vCenter Server, se detienen los mensajes rsyslog de vCenter Server. El servicio del plano de control de carga de trabajo detecta el cambio y lo propaga a cada máquina virtual del plano de control en cada Supervisor y detiene también los flujos de máquina virtual del plano de control.

Pasos de configuración

Realice los siguientes pasos para configurar la transmisión de rsyslog para máquinas virtuales del plano de control de Supervisor:

1 Configure un receptor rsyslog aprovisionando una máquina que:

  - Ejecuta el servicio rsyslog en modo receptor. Consulte el ejemplo Recuperar grandes cantidades de mensajes con alto rendimiento en la documentación de rsyslog.
  - Hay suficiente espacio de almacenamiento para alojar grandes cantidades de datos de registro.
  - Tiene conectividad de red para recibir datos de vCenter Server y las máquinas virtuales del plano de control de Supervisor.

2 Inicie sesión en la interfaz de administración del dispositivo de vCenter Server en *https://<dirección de vCenter Server>:5480* como raíz.

3 Configure vCenter Server para transmitir al receptor rsyslog a través de la interfaz de administración de dispositivos de vCenter Server. Consulte Reenviar archivos de registro de vCenter Server al servidor syslog remoto.

La configuración de rsyslog de vCenter Server puede tardar unos minutos en aplicarse a las máquinas virtuales del plano de control de Supervisor. El servicio del plano de control de carga de trabajo en el dispositivo de vCenter Server sondea la configuración del dispositivo cada 5 minutos y la propaga a todos los Supervisores disponibles. La cantidad de tiempo necesaria para que se complete la propagación depende de la cantidad de Supervisores en su entorno. En caso de que algunas de las máquinas virtuales del plano de control de los Supervisores tengan un estado incorrecto o realicen otra operación, el servicio del plano de control de carga de trabajo volverá a intentar aplicar la configuración de rsyslog hasta que se realice correctamente.

Inspeccionar registros de los componentes de máquinas virtuales del plano de control

El rsyslog de las máquinas virtuales del plano de control de Supervisor inserta etiquetas en los mensajes de registro que indican el componente de origen de estos mensajes de registro.

Etiquetas de registro	Descripción

`vns-control-plane-pods <pod_name>/<instance_number>.log`	Registros que se originaron desde pods de Kubernetes en máquinas virtuales del plano de control. Por ejemplo:
	`vns-control-plane-pods etcd/0.log`
	o
	`vns-control-plane-pods nsx-ncp/573.log`

`vns-control-plane-imc`	Registros de configuración inicial de las máquinas virtuales del plano de control.
`vns-control-plane-boostrap`	Registros de arranque de la implementación del plano de control de los nodos de Kubernetes.
`vns-control-plane-upgrade-logs`	Registros de revisiones de nodos del plano de control y actualizaciones de versiones secundarias.
`vns-control-plane-svchost-logs`	Registros de agente o host del servicio de nivel de sistema de la máquina virtual del plano de control.
`vns-control-plane-update-controller`	Sincronizador de estado deseado del plano de control y registro de vRealize.
`vns-control-plane-compact-etcd-logs`	Registros para mantener la compactación del almacenamiento del servicio etcd del plano de control.

Solucionar errores de compatibilidad del clúster para habilitar la administración de cargas de trabajo

Siga estos consejos para la solución de problemas si el sistema indica que el clúster de vSphere no es compatible con la habilitación de la administración de cargas de trabajo.

Problema

La página **Administración de cargas de trabajo** indica que el clúster de vCenter es incompatible cuando se intenta habilitar la administración de cargas de trabajo.

Causa

Esto puede deberse a varios motivos. En primer lugar, asegúrese de que el entorno cumpla con los requisitos mínimos para habilitar la administración de cargas de trabajo:

- Licencia válida: VMware vSphere 7 Enterprise Plus con el complemento para Kubernetes
- Al menos dos hosts ESXi
- DRS totalmente automatizado
- vSphere HA
- vSphere Distributed Switch 7.0
- Suficiente capacidad de almacenamiento

Si el entorno cumple con estos requisitos previos, pero el clúster de vCenter de destino no es compatible, utilice la CLI del centro de datos (Datacenter CLI, DCLI) de VMware para identificar los problemas.

Solución

1 SSH a vCenter Server.
2 Inicie sesión como usuario raíz.
3 Ejecute el comando `dcli` para mostrar la ayuda de la CLI del centro de datos de VMware.
4 Enumere los clústeres de vCenter disponibles ejecutando el siguiente comando de DCLI.

```
dcli com vmware vcenter cluster list
```

Por ejemplo:

```
dcli +username VI-ADMIN-USER-NAME +password VI-ADMIN-PASSWORD com vmware vcenter cluster
list
```

Resultado de ejemplo:

```
|-----------|---------|------------|----------|
|drs_enabled|cluster  |name        |ha_enabled|
|-----------|---------|------------|----------|
|True       |domain-d7|vSAN Cluster|True      |
|-----------|---------|------------|----------|
```

5 Compruebe la compatibilidad del clúster de vCenter ejecutando el siguiente comando de DCLI.

```
dcli com vmware vcenter namespacemanagement clustercompatibility list
```

Por ejemplo:

```
dcli +username VI-ADMIN-USER-NAME +password VI-ADMIN-PASSWORD com vmware vcenter
namespacemanagement clustercompatibility list
```

El siguiente resultado de ejemplo indica que, en el entorno, falta un conmutador VDS de NSX compatible.

```
|---------|----------|----------------------------------------------------------------------
-------------------|
|cluster  |compatible|
incompatibility_reasons                                                                |
|---------|----------|----------------------------------------------------------------------
-------------------|
|domain-d7|False     |Failed to list all distributed switches in vCenter 2b1c1fa5-
e9d4-45d7-824c-fa4176da96b8.|
|         |          |Cluster domain-d7 is missing compatible NSX
VDS.                                         |
|---------|----------|----------------------------------------------------------------------
-------------------|
```

6 Ejecute más comandos de DCLI según sea necesario para determinar otros problemas de compatibilidad. Además de errores de NSX, otros motivos comunes de incompatibilidad son los problemas de conectividad de DNS y NTP.

7 Para solucionar el problema, siga los pasos que se indican a continuación.

   a Ponga en cola el archivo `wcpsvc.log`. Consulte Poner en cola el archivo de registro de administración de cargas de trabajo.

   b Desplácese hasta la página **Administración de cargas de trabajo** y haga clic en **Habilitar**.

Poner en cola el archivo de registro de administración de cargas de trabajo

Poner en cola el archivo de registro de administración de cargas de trabajo puede ayudar a solucionar problemas de habilitación y corregir errores de implementación de Supervisor.

Solución

1. Establezca una conexión SSH con vCenter Server Appliance.
2. Inicie sesión como usuario `root`.
3. Ejecute el comando `shell`.

   Verá lo siguiente:

   ```
   Shell access is granted to root
   root@localhost [ ~ ]#
   ```

4. Ejecute el comando siguiente para poner el registro en cola.

   ```
   tail -f /var/log/vmware/wcp/wcpsvc.log
   ```

Solucionar problemas de redes 15

Para solucionar los posibles problemas de redes y equilibradores de carga, habilite el Supervisor.

Lea los siguientes temas a continuación:

Registrar vCenter Server en NSX Manager

En determinadas circunstancias, es posible que deba volver a registrar la instancia de OIDC de vCenter Server en NSX Manager (por ejemplo, cuando el FQDN o el PNID de vCenter Server cambian).

Procedimiento

1 Conéctese al dispositivo vCenter Server mediante SSH.

2 Ejecute el comando `shell`.

3 Para obtener la huella digital de vCenter Server, ejecute el siguiente comando:

```
- openssl s_client -connect vcenterserver-FQDN:443 </dev/null 2>/dev/null | openssl x509
-fingerprint -sha256 -noout -in /dev/stdin
```

Se mostrará la huella digital. Por ejemplo, `08:77:43:29:E4:D1:6F:29:96:78:5F:BF:D6:45:21:F4:0E:3B:2A:68:05:99:C3:A4:89:8F:F2:0B:EA:3A:BE:9D`

4 Copie la huella digital SHA256 y elimine los dos puntos.

`08774329E4D16F2996785FBFD64521F40E3B2A680599C3A4898FF20BEA3ABE9D`

5 Para actualizar la instancia de OIDC de vCenter Server, ejecute el siguiente comando:

```
curl --location --request POST 'https://<NSX-T_ADDRESS>/api/v1/trust-management/oidc-uris'
\
    --header 'Content-Type: application/json' \
    --header 'Authorization: Basic <AUTH_CODE>' \
```

```
    --data-raw '{
 "oidc_type": "vcenter",
     "oidc_uri": "https://<VC_ADDRESS>/openidconnect/vsphere.local/.well-known/openid-
configuration",
     "thumbprint": "<VC_THUMBPRINT>"
    }'
```

No se puede cambiar la contraseña de NSX Appliance

Es posible que no pueda cambiar la contraseña de NSX Appliance para los usuarios `root`, `admin` o `audit`.

Problema

Puede que se produzcan errores en los intentos de cambiar la contraseña de NSX Appliance para los usuarios `root`, `admin` o `audit` en vSphere Client.

Causa

Durante la instalación de NSX Manager, el procedimiento solo acepta una contraseña para las tres funciones. Se podría producir un error al intentar cambiar esta contraseña más tarde.

Solución

- Utilice las API de NSX para cambiar las contraseñas.

  Para obtener más información, consulte https://kb.vmware.com/s/article/70691 y la *Guía de administración de NSX*.

Solucionar problemas de flujos de trabajo con errores e instancias de NSX Edge inestables

Si se produce un error en los flujos de trabajo o las instancias de NSX Edge son inestables, puede realizar los pasos de solución de problemas.

Problema

Al cambiar la configuración del grupode puertos distribuidos en vSphere Client, se pueden producir errores en los flujos de trabajo y las instancias de NSX Edge pueden volverse inestables.

Causa

Por diseño, no se permite la eliminación ni la modificación de los grupos de puertos distribuidos para la superposición y el vínculo superior que se crearon durante la fase de configuración del clúster de NSX Edge de los ajustes del clúster.

Solución

Si necesita cambiar la configuración de la VLAN o del grupo de direcciones IP de las instancias de NSX Edge, primero debe eliminar los elementos de NSX y la configuración de vSphere IaaS control plane del clúster.

Para obtener información sobre cómo eliminar elementos de NSX, consulte la *Guía de instalación de NSX*.

Recopilar paquetes de soporte para la solución de problemas de NSX

Puede recopilar paquetes de soporte en los nodos de clúster y tejido registrados para solucionar problemas y descargar los paquetes en su máquina o cargarlos en un servidor de archivos.

Si decide descargar los paquetes en su máquina, obtendrá un solo archivo de almacenamiento compuesto por un archivo de manifiesto y paquetes de soporte para cada nodo. Si elige cargar los paquetes en un servidor de archivos, el archivo de manifiesto y los paquetes individuales se cargan en el servidor de archivos por separado

Procedimiento

1. Desde el navegador, inicie sesión con privilegios de administrador en un NSX Manager.
2. Seleccione **Sistema > Paquete de soporte**.
3. Seleccione los nodos de destino.

   Los tipos de nodos disponibles son **Nodos de administración** , **Edge**, **hosts** y **Puertas de enlace de nube pública**.
4. (opcional) Especifique la antigüedad del registro en días para excluir los registros que sean más antiguos que la cantidad especificada de días.
5. (opcional) Alterne el conmutador que indica si se deben incluir o excluir los registros de auditoría y los archivos principales.

   Nota Estos pueden contener información confidencial, como contraseñas o claves de cifrado.
6. (opcional) Active la casilla de verificación para cargar los paquetes a un servidor de archivos.
7. Haga clic en **Iniciar la recopilación de paquetes** para iniciar la recopilación de paquetes de soporte.

   La cantidad de archivos de registro de cada nodo determina el tiempo que se tarda en recopilar paquetes de soporte.
8. Supervise el estado del proceso de recopilación.

   La pestaña **Estado** muestra el progreso de la recopilación de paquetes de soporte.
9. Haga clic en **Descargar** para descargar el paquete si la opción para enviarlo a un servidor de archivos no se ha establecido

Recopilar archivos de registro para NSX

Puede recopilar los registros que se encuentran en los componentes de vSphere IaaS control plane y NSX para detectar errores y solucionarlos. Los archivos de registro pueden solicitarse a través del soporte de VMware.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Recopile los siguientes archivos de registro.

Archivo de registro	Descripción
/var/log/vmware/wcp/wcpsvc.log	Contiene información relacionada con la habilitación de vSphere IaaS control plane.
/var/log/vmware/wcp/nsxd.log	Contiene información relacionada con la configuración de los componentes de NSX.

3 Inicie sesión en NSX Manager.

4 Recopile el archivo `/var/log/proton/nsxapi.log` para obtener información sobre el error que NSX Manager devuelve cuando se produce un error en una operación de vSphere IaaS control plane específica.

Reiniciar el servicio WCP si la dirección IP, la huella digital o el certificado de administración de NSX cambian

Si la dirección IP, la huella digital o el certificado de administración de NSX cambian después de instalar vSphere IaaS control plane, debe reiniciar el servicio `WCP`.

Reiniciar el servicio vSphere IaaS control plane si el certificado de NSX cambia

Actualmente, según los requisitos de vSphere IaaS control plane, si la huella digital o el certificado de NSX o la dirección IP de NSX cambian, es necesario reiniciar el servicio `WCP` para que se implemente el cambio. Si se realiza el cambio sin reiniciar el servicio, se produce un error en la comunicación entre vSphere IaaS control plane y NSX, y se pueden presentar ciertos síntomas, como que NCP ingrese en la etapa CrashLoopBackoff o que los recursos del Supervisor no se puedan implementar.

Para reiniciar el servicio `WCP`, utilice `vmon-cli`.

1 Ejecute SSH en vCenter Server e inicie sesión como usuario raíz.

2 Ejecute el comando `shell`.

3 Ejecute el comando `vmon-cli -h` para ver las opciones y la sintaxis de uso.

4 Ejecute el comando `vmon-cli -l` para ver el proceso de `wcp`.

   Verá el servicio `wcp` en la parte inferior de la lista.

5 Ejecute el comando `vmon-cli --restart wcp` para reiniciar el servicio `wcp`.

Verá el mensaje `Completed Restart service request`.

6 Ejecute el comando `vmon-cli -s wcp` y compruebe que se haya iniciado el servicio `wcp`.

Por ejemplo:

```
root@localhost [ ~ ]# vmon-cli -s wcp
Name: wcp
Starttype: AUTOMATIC
RunState: STARTED
RunAsUser: root
CurrentRunStateDuration(ms): 22158
HealthState: HEALTHY
FailStop: N/A
MainProcessId: 34372
```

Recopilar paquetes de soporte para la solución de problemas de NSX Advanced Load Balancer

Para solucionar problemas de NSX Advanced Load Balancer, puede recopilar paquetes de soporte. Es posible que el Soporte técnico de VMware solicite los paquetes de soporte.

Cuando genere el paquete de soporte, obtendrá un único archivo descargable para los registros de depuración.

Procedimiento

1 En el panel de control de NSX Advanced Load Balancer Controller, haga clic en el menú situado en la esquina superior izquierda y seleccione **Administración**.

2 En la sección **Administración**, seleccione **Sistema**.

3 En la pantalla **Sistema**, seleccione **Soporte técnico**.

4 Para generar un paquete de diagnósticos, haga clic en **Generar soporte técnico**.

5 En la ventana **Generar soporte técnico**, seleccione **Registros de depuración** y haga clic en **Generar**.

6 Una vez generado el paquete, haga clic en el icono de descarga para descargarlo en su máquina.

Para obtener más información sobre la recopilación de registros, consulte https://avinetworks.com/docs/21.1/collecting-tech-support-logs/.

La configuración de NSX Advanced Load Balancer no se aplica

Cuando se implementa el Supervisor, la implementación no se completa y no se aplica la configuración de NSX Advanced Load Balancer.

Problema

La configuración de NSX Advanced Load Balancer no se aplica si proporciona un certificado firmado por una entidad de certificación (CA) privada.

Es posible que aparezca un mensaje de error con `Unable to find certificate chain` en los archivos de registro de uno de los pods de NCP que se ejecutan en el Supervisor.

1 Inicie sesión en la máquina virtual del Supervisor.

2 Enumere todos los pods con el comando `kubectl get pods -A`.

3 Obtenga los registros de todos los pods de NCP en el Supervisor.

   ```
   kubectl -n vmware-system-nsx logs nsx-ncp-<id> | grep -i alb
   ```

Causa

El SDK de Java se utiliza para establecer la comunicación entre NCP y NSX Advanced Load Balancer Controller. Este error se produce cuando el almacén de confianza NSX no está sincronizado con el almacén de confianza de certificados de Java.

Solución

1 Exporte el certificado de CA raíz desde NSX Advanced Load Balancer y guárdelo en NSX Manager.

2 Inicie sesión en NSX Manager como usuario raíz.

3 Ejecute los siguientes comandos de forma secuencial en todos los nodos de NSX Manager:

   ```
   keytool -importcert -alias startssl -keystore /usr/lib/jvm/jre/lib/security/cacerts
   -storepass changeit -file <ca-file-path>
   ```

   Si no se encuentra la ruta de acceso, ejecute `keytool -importcert -alias startssl -keystore /usr/java/jre/lib/security/cacerts -storepass changeit -file <ca-file-path>`

   ```
   sudo cp <ca-file-path> /usr/local/share/ca-certificates/
   sudo update-ca-certificates
   service proton restart
   ```

   Nota Puede realizar los mismos pasos para asignar un certificado de CA intermedia.

4 Espere a que finalice la implementación del Supervisor o, si no se produce la implementación, vuelva a implementarla.

El host ESXi no puede entrar en modo de mantenimiento

Cuando desea realizar una actualización, debe colocar un host ESXi en modo de mantenimiento.

Problema

El host ESXi no puede entrar en modo de mantenimiento y puede afectar a la actualización de ESXi y NSX.

Causa

Esto puede ocurrir si hay un motor de servicio en estado encendido en el host ESXi.

Solución

◆ Apague el motor de servicio para que el host ESXi pueda entrar en modo de mantenimiento.

Solucionar problemas de direcciones IP

Siga estos consejos de solución de problemas si tiene problemas con la asignación de direcciones IP externas.

Se pueden producir errores en las direcciones IP por los siguientes motivos:

- Los recursos de Kubernetes, como las puertas de enlace y la entrada, no obtienen una dirección IP externa del AKO.
- No es posible acceder a las direcciones IP externas que están asignadas a recursos de Kubernetes.
- Direcciones IP externas que están asignadas de forma incorrecta.

Los recursos de Kubernetes no obtienen una IP externa de la AKO

Este error se produce cuando AKO no puede crear el servicio virtual correspondiente en NSX Advanced Load Balancer Controller.

Compruebe si el pod del AKO se está ejecutando. Si el pod se está ejecutando, compruebe los registros del contenedor AKO para el error.

No es posible acceder a las direcciones IP externas asignadas a recursos de Kubernetes

Este problema puede ocurrir por los siguientes motivos:

- La dirección IP externa no está disponible inmediatamente, pero comienza a aceptar tráfico pocos minutos después de crearla. Esto ocurre cuando se activa la creación de un nuevo motor de servicio para la colocación de servicios virtuales.
- La IP externa no está disponible porque el servicio virtual correspondiente muestra un error.

Un servicio virtual podría indicar un error o aparecer en rojo si no hay servidores en el grupo. Esto puede ocurrir si el recurso de entrada o las puertas de enlace de Kubernetes no apuntan a un objeto de endpoint.

Para ver los endpoints, ejecute el comando `kubectl get endpoints -n <servce_namespace>` y solucione los problemas de la etiqueta del selector.

El grupo puede mostrar un estado de error cuando el monitor de estado muestra el estado de los servidores del grupo en rojo.

Realice uno de los siguientes pasos para resolver este problema:

- Compruebe si los servidores de grupo o los pods de Kubernetes están escuchando en el puerto configurado.
- Compruebe que no haya reglas de descarte en el firewall de NSX DFW que bloqueen el tráfico de entrada o salida en los motores de servicio.
- Asegúrese de que no haya directivas de red en el entorno de Kubernetes que bloqueen el tráfico de entrada o salida en los motores de servicio.

Entre los problemas del motor de servicio se incluyen los siguientes:

1 Se produce un error en la creación del motor de servicio.

   Se puede producir un error en la creación de motores de servicio por los siguientes motivos:

   - Se utiliza una licencia con recursos insuficientes en NSX Advanced Load Balancer Controller.
   - La cantidad de motores de servicio creados en un grupo de motores de servicio alcanzó el límite máximo.
   - La NIC de datos del motor de servicio no pudo adquirir la dirección IP.

2 Se produce un error en la creación del motor de servicio y aparece un mensaje de error del tipo `Insufficient licensable resources available`.

   Este error se produce si se utilizó una licencia con recursos insuficientes para crear el motor de servicio.

   Obtenga una licencia con mayor cuota de recursos y asígnela a la NSX Advanced Load Balancer Controller.

3 Se produce un error en la creación del motor de servicio y aparece un mensaje de error del tipo `Reached configuration maximum limit`.

   Este error se produce si el número de motores de servicio creados en un grupo de motores de servicio alcanzó el límite máximo.

   Para solucionar este error, realice los siguientes pasos:

   a En el panel de la NSX Advanced Load Balancer Controller, seleccione **Infraestructura > Recursos de nube > Grupo de motores de servicio**.

   b Busque el grupo de motores de servicio con el mismo nombre que el Supervisor en el que se produce el error del tráfico IP y haga clic en el icono **Editar**.

   c Configure un valor más alto para **Número de motores de servicio**.

4 La NIC de datos del motor de servicio no puede adquirir la dirección IP.

Este error puede producirse si el grupo de direcciones IP de DHCP se agotó por uno de los siguientes motivos:

- Se crearon demasiados motores de servicio para una implementación a gran escala.
- Si se elimina un motor de servicio directamente de la interfaz de usuario de NSX Advanced Load Balancer o vSphere Client. Esta eliminación no libera la dirección DHCP del grupo DHCP y da lugar a un error de asignación de CONCESIÓN.

Las direcciones IP externas no están asignadas correctamente

Este error se produce cuando dos entradas en espacios de nombres diferentes comparten el mismo nombre de host. Compruebe la configuración y que no se asigne el mismo nombre a dos entradas en espacios de nombres diferentes.

Solucionar problemas de errores de tráfico

Después de configurar NSX Advanced Load Balancer, se producen errores de tráfico.

Problema

Se pueden producir errores de tráfico cuando el endpoint del servicio de tipo LB se encuentra en un espacio de nombres diferente.

Causa

En entornos de vSphere IaaS control plane configurados con NSX Advanced Load Balancer, los espacios de nombres tienen una puerta de enlace de nivel 1 dedicada y cada puerta de enlace de nivel 1 tiene un segmento de motor de servicio con el mismo CIDR. Se pueden producir errores de tráfico si el servicio NSX Advanced Load Balancer se encuentra en un espacio de nombres y los endpoints se encuentran en un espacio de nombres diferente. El error se produce debido a que NSX Advanced Load Balancer asigna una IP externa al servicio y se produce un error en el tráfico a la IP externa.

Solución

- ◆ Para permitir el tráfico de norte a sur, cree una regla de firewall distribuido para permitir la entrada desde la IP de SNAT del espacio de nombres del servicio NSX Advanced Load Balancer.

Solución de problemas causados por la copia de seguridad y restauración de NSX

La copia de seguridad y restauración de NSX pueden provocar errores de tráfico en todas las direcciones IP externas que proporciona NSX Advanced Load Balancer.

Problema

Cuando se realiza una copia de seguridad y una restauración de NSX, se puede producir un error de tráfico.

Causa

Este error se produce cuando las NIC del motor de servicio no se activan de nuevo tras una restauración y, como resultado, el grupo de direcciones IP aparece como inactivo.

Solución

1 En el panel de control de NSX Advanced Load Balancer Controller, seleccione **Infraestructura > Nubes**.

2 Seleccione y guarde la nube sin realizar cambios y espere a que el estado cambie a verde.

3 Desactive todos los servicios virtuales.

   Espere a que la NSX Advanced Load Balancer Controller elimine las NIC obsoletas de todos los motores de servicio.

4 Habilite todos los servicios virtuales.

   Los estados de los servicios virtuales aparecen en verde.

   Si el error de tráfico persiste, vuelva a configurar las rutas estáticas en NSX Manager.

Segmentos de nivel 1 obsoletos después de la copia de seguridad y restauración de NSX

La copia de seguridad y restauración de NSX puede restaurar segmentos de nivel 1 obsoletos.

Problema

Después de un procedimiento de copia de seguridad y restauración de NSX, los segmentos de nivel 1 obsoletos que tienen NIC del motor de servicio no se limpian.

Causa

Cuando se elimina un espacio de nombres después de una copia de seguridad de NSX, la operación de restauración restaura los segmentos de nivel 1 obsoletos que están asociados con las NIC del motor de servicio de NSX Advanced Load Balancer Controller.

Solución

1 Inicie sesión en NSX Manager.

2 Seleccione **Redes > Segmentos**.

3 Busque los segmentos obsoletos que están asociados con el espacio de nombres eliminado.

4 Elimine las NIC obsoletas del motor de servicio en la sección **Puertos/Interfaces**.

VDS requerido para el tráfico del nodo de transporte del host

vSphere IaaS control plane requiere el uso de un conmutador virtual distribuido (Virtual Distributed Switch, VDS) de vSphere 8,0 para el tráfico del nodo de transporte del host. No

puede utilizar el VDS de NSX (N-VDS) para el tráfico del nodo de transporte del host con vSphere IaaS control plane.

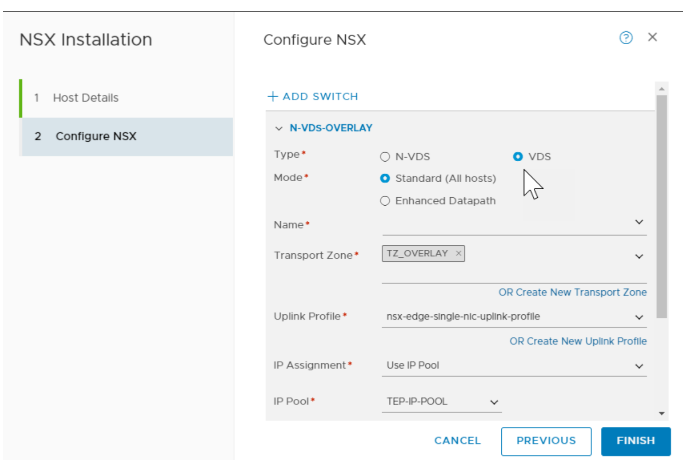
Se requiere VDS

vSphere IaaS control plane requiere un VDS convergente que admita el tráfico de vSphere y de NSX en el mismo VDS. En las versiones anteriores de vSphere y NSX, existe un VDS (o VSS) para el tráfico de vSphere y un N-VDS para el tráfico de NSX. Esta configuración no es compatible en vSphere IaaS control plane. Si intenta habilitar la administración de cargas de trabajo usando un N-VDS, el sistema informa que el clúster de vCenter no es compatible. Para obtener más información, consulte Solucionar errores de compatibilidad del clúster para habilitar la administración de cargas de trabajo.

Para utilizar un VDS convergente, cree un vDS de vSphere 8.0 mediante vCenter y, en NSX, especifique este VDS al preparar los hosts ESXi como nodos de transporte. No alcanza con disponer de VDS-DSwitch en el lado de vCenter. Es necesario configurar VDS-DSwitch 8.0 con un perfil de nodo de transporte de NSX, tal como se describe en el tema Crear un perfil de nodo de transporte y se muestra a continuación.

Para obtener más información sobre cómo preparar hosts ESXi como nodos de transporte, consulte https://kb.vmware.com/s/article/95820 y Preparar hosts ESXi como nodos de transporte en la documentación de NSX.

Figura 15-1. Configuración de VDS en NSX



Si actualizó a vSphere 8.0 y NSX 4.x desde versiones anteriores, debe desinstalar el N-VDS de cada nodo de transporte de ESXi y volver a configurar cada host con una instancia de VDS. Póngase en contacto con VMware Global Support Service para obtener instrucciones.

Solucionar problemas en vSphere IaaS control plane

16

Siga las prácticas recomendadas y las técnicas de solución de problemas siguientes para su infraestructura en vSphere IaaS control plane.

Lea los siguientes temas a continuación:

Prácticas recomendadas y solución de problemas de almacenamiento

Utilice las siguientes prácticas recomendadas y técnicas de solución de problemas en su entorno de almacenamiento de vSphere IaaS control plane.

Usar reglas antiafinidad para máquinas virtuales del plano de control en almacenes de datos que no sean de vSAN

Cuando use almacenes de datos que no sean de vSAN en el clúster con vSphere IaaS control plane, coloque las tres máquinas virtuales del plano de control en distintos almacenes de datos por motivos de disponibilidad.

Debido a que las máquinas virtuales del plano de control son administradas por el sistema, no se las puede migrar manualmente. Utilice una combinación de un clúster de almacenes de datos y Storage DRS para volver a equilibrar las máquinas virtuales del plano de control y colocarlas en almacenes de datos independientes.

Procedimiento

1 En vSphere Client, cree un clúster de almacenes de datos.

   a Vaya a los centros de datos.

   b Haga clic con el botón secundario en el objeto del centro de datos y seleccione **Nuevo clúster de almacenes de datos**.

c Asigne un nombre al clúster de almacenes de datos y asegúrese de que **Activar Storage DRS** esté habilitado.

d Establezca el nivel de automatización del clúster en **Sin automatización (modo manual)**.

e Deje la configuración predeterminada del tiempo de ejecución de Storage DRS.

f Seleccione el clúster de ESXi habilitado con vSphere IaaS control plane.

g Seleccione todos los almacenes de datos compartidos para agregar al clúster de almacenes de datos.

h Haga clic en **Finalizar**.

2 Defina las reglas de Storage DRS para las máquinas virtuales del plano de control.

a Desplácese hasta el clúster de almacenes de datos.

b Haga clic en la pestaña **Configurar** y en **Reglas**, en **Configuración**.

c Haga clic en el icono **Agregar** e introduzca el nombre para la regla.

d Asegúrese de que **Habilitar regla** esté activado.

e Establezca **Tipo de regla** en **Antiafinidad de máquina virtual**.

f Haga clic en el icono **Agregar** y seleccione las tres máquinas virtuales del plano de control de supervisor.

g Haga clic en **Aceptar** para finalizar la configuración.

3 Cree reemplazos de máquinas virtuales.

a Desplácese hasta el clúster de almacenes de datos.

b Haga clic en la pestaña **Configurar** y en **Reemplazos de máquinas virtuales**, en **Configuración**.

c Haga clic en el icono **Agregar** y seleccione las tres máquinas virtuales del plano de control.

d Para habilitar el nivel de automatización de Storage DRS, active la casilla de verificación **Reemplazar** y establezca el valor en **Totalmente automatizado**.

e Haga clic en **Finalizar**.

Resultados

Esta tarea solo habilita Storage DRS para las máquinas virtuales del plano de control y vuelve a equilibrar las máquinas virtuales para que se encuentren en almacenes de datos diferentes.

Una vez que se llevan a cabo las operaciones de Storage vMotion, puede eliminar las reglas y los reemplazos de SDRS, deshabilitar Storage DRS y eliminar el clúster de almacenes de datos.

La directiva de almacenamiento eliminada de vSphere sigue apareciendo como clase de almacenamiento Kubernetes

Cuando se utiliza vSphere Client para eliminar la directiva de almacenamiento de VMware vCenter o un espacio de nombres en el Supervisor, la clase de almacenamiento coincidente permanece en el entorno de Kubernetes, pero no se puede utilizar.

Problema

Si ejecuta el comando **`kubectl get sc`**, el resultado seguirá mostrando la clase de almacenamiento como disponible en el espacio de nombres. Sin embargo, esta no se podrá usar. Por ejemplo, se produce un error al intentar usar la clase de almacenamiento para una nueva notificación de volumen persistente.

Si una implementación de Kubernetes ya utiliza la clase de almacenamiento, es posible que la implementación se comporte de forma impredecible.

Solución

1. Para comprobar qué clases de almacenamiento hay en el espacio de nombres, ejecute el comando **`kubectl describe namespace`** ***`namespace_name`***.

   La salida de este comando no muestra la clase de almacenamiento si se elimina la directiva de almacenamiento coincidente.

2. Si una implementación ya utiliza la clase de almacenamiento, restaure la clase de almacenamiento.

   a. Utilice vSphere Client para crear una nueva directiva de almacenamiento con el mismo nombre que la directiva que eliminó.

      Por ejemplo, si eliminó la directiva *Oro*, asigne el nombre *Oro* a la nueva directiva. Consulte Crear directivas de almacenamiento para vSphere with Tanzu en *Instalar y configurar el plano de control de IaaS de vSphere*.

   b. Asigne la directiva al espacio de nombres.

      Consulte Cambiar la configuración de almacenamiento en un espacio de nombres en *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

      Después de asignar la directiva al espacio de nombres, vSphere IaaS control plane elimina la clase de almacenamiento anterior y crea una clase de almacenamiento coincidente con el mismo nombre.

Usar almacenamiento externo con vSAN Direct

Al utilizar vSAN Direct en el entorno vSphere IaaS control plane, se puede usar un almacenamiento compartido externo para almacenar máquinas virtuales internas de administración y otros metadatos.

Problema

Al implementar un clúster de vSAN Direct homogéneo, debe crear un almacén de datos de vSAN replicado en cada host ESXi del clúster para almacenar las máquinas virtuales del plano de control de Supervisor y otros metadatos. El almacén de datos de vSAN consume espacio, requiere un controlador de E/S adicional en cada host y limita la configuración de hardware en la que vSAN Direct puede ser compatible.

En lugar de configurar el almacén de datos de vSAN, puede usar el almacenamiento compartido externo para almacenar las máquinas virtuales internas de administración y otros metadatos.

Solución

1 Si vSAN o vSAN Direct se implementaron en hosts ESXi del clúster, borre los hosts de cualquier configuración.

   a Elimine los discos asignados a vSAN o vSAN Direct. Consulte Quitar grupos de discos o dispositivos de vSAN en *Administrar VMware vSAN*.

   b (opcional) Utilice el script a fin de etiquetar discos en los hosts para vSAN Direct. Consulte Usar un script para etiquetar dispositivos de almacenamiento para vSAN Direct.

2 Utilice VMware Cloud Foundation para crear un dominio de carga de trabajo con almacenamiento externo.

   Asegúrese de seleccionar una de las opciones de almacenamiento, como NFS, vVols o canal de fibra. Solo se puede seleccionar una de estas opciones.

   Para obtener más información, consulte *Trabajo con dominios de carga de trabajo* en la Documentación de VMware Cloud Foundation.

   Este paso implementa un dominio de carga de trabajo con vCenter Server y los hosts ESXi especificados. El almacenamiento externo se monta en todos los hosts y se agrega al clúster predeterminado.

3 Habilite vSAN.

   Asegúrese de que no haya discos reclamados para vSAN.

   Para obtener más información, consulte Habilitar vSAN en un clúster existente en *Administrar VMware vSAN*.

   Este paso crea un almacén de datos de vSAN de cero bytes con la red de vSAN. No se usan discos locales para vSAN.

4 Reclame los discos locales en los hosts para vSAN Direct.

   Para obtener información, consulte Crear un almacén de datos de vSAN Direct en *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

   Por cada dispositivo que reclame, vSAN Direct creará un almacén de datos independiente.

5 Cree directivas de almacenamiento para vSAN Direct.

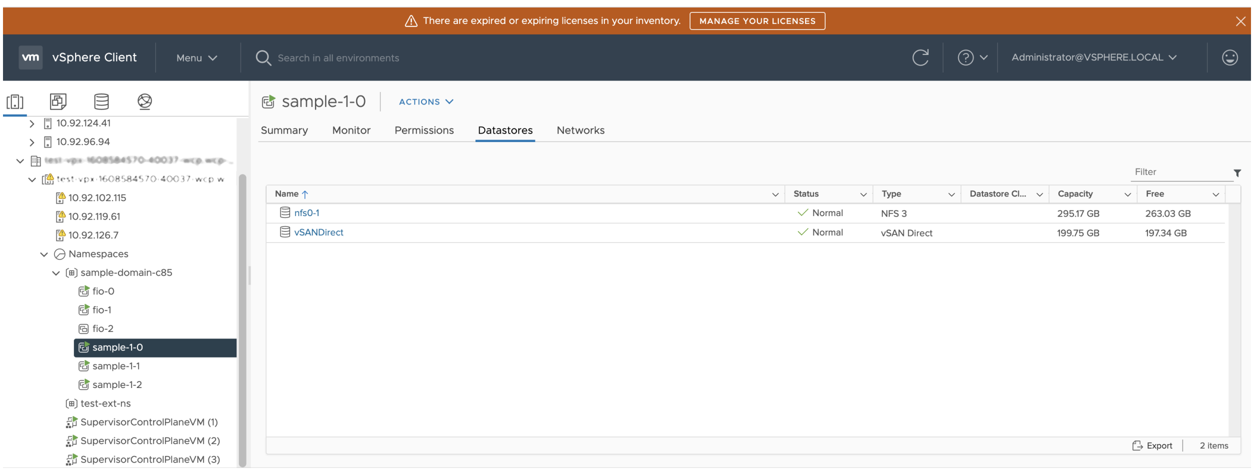
   Para obtener información, consulte Crear una directiva de almacenamiento de vSAN Direct en *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

6 Habilite Supervisor.

Para obtener información, consulte el documento *Instalar y configurar el plano de control de IaaS de vSphere*.

Ejemplo

En este ejemplo, una configuración incluye almacenamiento NFS externo y un almacén de datos de vSAN Direct. Las máquinas virtuales de plano de control de pods de vSphere se ejecutan en el almacenamiento NFS externo. Las notificaciones de volumen persistente se ejecutan en vSAN Direct.



Solucionar problemas de actualización de la topología de red

Cuando instala la versión 7.0 Update 1c de vSphere IaaS control plane o actualiza el Supervisor desde la versión 7.0 Update 1 a la versión 7.0 Update 1c, la topología de red se actualiza desde una topología de puerta de enlace de nivel 1 única a una topología que tiene una puerta de enlace de nivel 1 para cada espacio de nombres dentro del Supervisor.

Puede solucionar los problemas que puede encontrar durante la actualización.

Error en la comprobación previa de la actualización debido a que no hay suficiente capacidad en el equilibrador de carga de Edge

Se produce un error en la comprobación previa de la actualización y el mensaje de error indica que no el equilibrador de carga no tiene suficiente capacidad.

Problema

El proceso de comprobación previa a la actualización genera un error con un mensaje que indica que la capacidad del equilibrador de carga es menor que la capacidad que necesita el Supervisor.

Solución

Realice uno de los siguientes pasos para solucionar el problema:

- Para forzar la actualización, haga clic en el botón **Forzar actualización** en el mensaje de error o utilice la línea de comandos vCenter Server con la marca `--ingnore-precheck-warnings true`.

  Nota Esta solución se recomienda solo si el clúster de Edge puede admitir las cargas de trabajo de espacios de nombres existentes. De lo contrario, se podrían omitir estas cargas de trabajo durante la actualización.

- Elimine las cargas de trabajo no utilizadas.
- Agregue otros nodos de Edge al clúster.

Se omitieron espacios de nombres de cargas de trabajo del Supervisor durante la actualización

Durante la actualización del Supervisor no se actualizaron algunas cargas de trabajo del espacio de nombres.

Problema

La actualización del Supervisor se realiza correctamente pero se omiten algunas cargas de trabajo del espacio de nombres durante la actualización. Los recursos de Kubernetes indican que los recursos son insuficientes y el estado de la puerta de enlace de nivel 1 que se acaba de crear es `ERROR`.

Causa

La capacidad del equilibrador de carga no es suficiente para admitir las cargas de trabajo.

Solución

Realice uno de los siguientes pasos para solucionar el problema:

- Elimine las cargas de trabajo que no se utilicen, reinicie NCP y vuelva a ejecutar la actualización.
- Agregue nodos de Edge adicionales al clúster y active una reasignación a la puerta de enlace de nivel 1. Reinicie NCP y vuelva a ejecutar la actualización.

Servicio de equilibrador de carga omitido durante la actualización

Durante la actualización del Supervisor, algunos servicios del equilibrador de carga no se actualizan.

Problema

La actualización del Supervisor se realiza correctamente, pero se omiten algunos servicios del equilibrador de carga de Kubernetes durante la actualización.

Causa

La cantidad de servicios de tipo de equilibrador de carga de Kubernetes en las cargas de trabajo del Supervisor y el clúster de Tanzu Kubernetes asociado supera el límite de servidores virtuales de NSX Edge.

Solución

Elimine las cargas de trabajo que no se utilicen, reinicie NCP y vuelva a ejecutar la actualización.

Apagar e iniciar el dominio de carga de trabajo de vSphere IaaS control plane

Para evitar la pérdida de datos y mantener operativos los componentes y las cargas de trabajo del entorno de vSphere IaaS control plane, debe seguir el orden especificado al apagar o iniciar los componentes.

Por lo general, las operaciones de inicio y apagado se realizan después de aplicar una revisión, actualizar o restaurar el entorno de vSphere IaaS control plane.

La solución vSphere IaaS control plane, incluidos los clústeres de Tanzu Kubernetes aprovisionados por Tanzu Kubernetes Grid, forma parte del centro de datos definido por software (SDDC) de vSphere. Por lo tanto, debe tener en cuenta toda la pila de infraestructura de vSphere al apagar e iniciar el entorno de vSphere IaaS control plane. Consulte el siguiente conjunto validado de procedimientos para el apagado y el inicio del SDDC de vSphere incluido vSphere IaaS control plane:

- SDDC de vSphere incluido el procedimiento de apagado de vSphere IaaS control plane
- SDDC de vSphere incluido el procedimiento de inicio de vSphere IaaS control plane

Recopilar el paquete de soporte para un Supervisor

Consulte cómo recopilar un paquete de soporte para un Supervisor. Puede recopilar un paquete de soporte incluso si el Supervisor está en estado de error o de configuración.

Requisitos previos

- Su cuenta de usuario debe tener el privilegio **Global.Diagnósticos**.

Procedimiento

1 Inicie sesión en su entorno de vSphere IaaS control plane mediante vSphere Client.
2 Seleccione **Menú > Administración de cargas de trabajo**.
3 Seleccione la pestaña **Supervisores**.
4 Seleccione el Supervisor de destino.
5 Haga clic en **Exportar registros**.

Resultados

Una vez que haya recopilado el paquete de soporte, consulte el siguiente artículo de la base de conocimientos: Cómo cargar información de diagnóstico para VMware a través del portal de FTP seguro: http://kb.vmware.com/kb/2069559.